Unconditional security from noisy quantum storage

Robert König[1], Stephanie Wehner[1,3], and Jürg Wullschleger[2]

[1] *Caltech, Institute for Quantum Information, Pasadena CA 91125, USA*

[2] *University of Bristol, Department of Mathematics, Bristol BS8 1TW, UK*

[3] *Centre for Quantum Technologies, National University of Singapore, 117543 Singapore*

July 20, 2010

Abstract

We consider the implementation of two-party cryptographic primitives based on the sole assumption that no large-scale reliable quantum storage is available to the cheating party. We construct novel protocols for oblivious transfer and bit commitment, and prove that realistic noise levels provide security even against the most general attack. Such unconditional results were previously only known in the so-called bounded-storage model which is a special case of our setting. Our protocols can be implemented with present-day hardware used for quantum key distribution. In particular, no quantum storage is required for the honest parties.

Contents

1   The noisy-storage model: definition and results

1.1   Motivation: security from *physical* assumptions

The security of most cryptographic systems currently in use is based on the premise that a certain computational problem is hard to solve for the adversary. Concretely, this relies on the assumption that the adversary's computational resources are limited, and the underlying problem is hard in some precise complexity-theoretic sense. While the former assumption may be justified in practice, the latter statement is usually an unproven mathematical conjecture. In contrast, quantum cryptographic schemes are designed in such a way that they provide security based solely on the validity of quantum physics. No assumptions on the adversary's computational power nor the validity of some complexity-theoretic statements are needed.

Unfortunately, not even the laws of quantum physics allow us to realize all desirable cryptographic functionalities without further assumptions [37, 44, 39, 38, 45]. An example of such a functionality is (fully randomized) oblivious transfer, where Alice receives two random strings S_0, S_1, while Bob receives one of the strings S_C together with the index C. Security for this primitive means that neither Alice nor Bob can obtain any information beyond this specification. A protocol which securely implements oblivious transfer is desirable because any two-party computation, such as secure identification, can be based on this building block [29, 23].

In light of this state of affairs, it is natural to consider other *physical* assumptions: Motivated by similar classical models [42, 43], the authors of [16, 15] and [60, 62, 55] propose to assume that the adversary's *quantum* storage is bounded and noisy, respectively. The assumption of bounded quantum storage deals with the noiseless case (but assumes a small amount of storage), whereas the noisy-storage model deals with the case of noise (but possibly a large amount of storage). Here, we introduce a more general point of view which incorporates both the amount of storage and noise. We refer to this simply as the *noisy-storage model*. The previously considered settings are special cases, as we will explain below.

Compared to the classical world, the assumption of limited and noisy quantum storage is particularly realistic in view of the present state of the art, and the considerable challenges faced when trying to build scalable quantum memories. Indeed, it is unknown whether it is physically possible to build noise free memories. Further motivation for considering noise as a resource for security over the mere assumption of bounded storage comes from the fact that the transfer of the state of a (photonic) qubit used during the execution of the protocol onto a different carrier used as a quantum memory (such as an atomic ensemble) is typically already noisy. At present, it is not even clear whether it is theoretically possible to close this gap in a quantum mechanical world, or if this transformation is *inherently* noisy.

2

1.2 Contribution and methods

Here, we consider the noisy-storage model which was previously introduced in [60, 62, 55] where it appeared in a slightly more specialized form. All previous security proofs in this model required additional assumptions beyond having noise. In particular, in the analysis of [62], the adversary was restricted to performing individual attacks using product measurements on the qubits received in the protocol. This is a significant restriction as multi-qubit measurements are possible even today, and can be compared to an analysis of quantum key distribution [4] where the eavesdropper is restricted to measuring each qubit individually. We provide a fully general proof of security against arbitrary attacks that bit-commitment and oblivious transfer can be achieved in the general noisy-storage model which encompasses and extends all previously considered settings [16, 15, 60, 62, 55]. As a side effect, we thereby also obtain significantly improved parameters for the special case of bounded storage.

In order to obtain this result, we require a number of methods that have not been used before either in the noisy- or bounded-quantum-storage setting.

- We formally relate the security of our protocols to the problem of sending information through the noisy-storage channel. This is very intuitive, and much more natural than previous approaches such as the restriction to individual attacks in the noisy-storage model [62], or the assumption of bounded storage [16]. More specifically, we show that a sufficient condition for security is that the number of classical bits that can be sent through the noisy-storage channel is limited. We introduce our generalized model in Section 1.3, and state our result in Section 1.4.

- We introduce a novel cryptographic primitive called weak string erasure (see Section 3) that may be of independent interest. We provide a simple quantum protocol that securely realizes weak string erasure in the noisy-storage model, in which the honest parties do not require any quantum memory at all to execute the protocol. Our protocol can be implemented with present-day technology. In our security proof, we require information-theoretic tools such as the recently proven strong converse for channel coding [36].

- We construct new protocols for bit commitment and oblivious transfer based on weak string erasure, and prove security against arbitrary attacks. Our protocols are purely classical, merely using the simple quantum primitive of weak string erasure which is a conceptually appealing feature. We thereby make use of various techniques such as error-correcting codes, privacy amplification, interactive hashing and min-entropy sampling with respect to a quantum adversary.

Our work raises many immediate open questions, and has already sparked several other works which we discuss in Section 6.

1.3 The noisy-storage model

Let us now describe more formally what we mean by a noisy quantum memory. We think of a device whose input states are in some Hilbert space $\mathcal{H}_{in}$. A state ρ stored in the device decoheres over time. That is, the content of the memory after some time t is a state $\mathcal{F}_t(\rho)$, where $\mathcal{F}_t : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$ is a completely positive trace-preserving map corresponding to the noise in the memory. Since the amount of noise may of course depend on the storage time, the behaviour of the storage is completely described by the family of maps $\{\mathcal{F}_t\}_{t>0}$. We will make the *minimal* assumption that the noise is Markovian, that is, the family $\{\mathcal{F}_t\}_{t>0}$ is a continuous one-parameter semigroup

$$\mathcal{F}_0 = \mathbb{I} \qquad \text{and} \qquad \mathcal{F}_{t_1+t_2} = \mathcal{F}_{t_1} \circ \mathcal{F}_{t_2} . \tag{1}$$

This tells us that the noise in storage only increases with time, and is essential to ensure that the adversary cannot gain any information by delaying the readout [1]. This is the only restriction imposed on the adversary

---

[1]This property is implicitly assumed in [62].

3

who may otherwise be all-powerful. In particular, we allow that all his actions are instantaneous, including computation, communication, measurement and state preparation.

How can we hope to obtain security in such a model? In our protocol, we will introduce certain time delays Δt which force any adversary to use his storage device for a time at least Δt. Our assumptions imply that the best an adversary can do is to read out the information from the device immediately after time Δt, as any further delay will only degrade his information further. We can thus focus on the channel $\mathcal{F} = \mathcal{F}_{\Delta t}$ when analyzing security instead of the family $\{\mathcal{F}_t\}_{t \geq 0}$. Note that since the adversaries actions are assumed to be instantaneous, he can use any error-correcting code even if the best encoding and decoding procedure may be difficult to perform. Summarizing, our model assumes that

- The adversary has unlimited classical storage, and (quantum) computational resources.

- Whenever the protocol requires the adversary to wait for a time Δt, he has to measure/discard all his quantum information except what he can encode (arbitrarily) into $\mathcal{H}_{in}$. This information then undergoes noise described by $\mathcal{F}$.

To see how previously analyzed cases fit into our model, note that the bounded-storage model corresponds to the case where $\mathcal{H}_{in}$ is of limited input dimension, and $\mathcal{F}$ is the identity on $\mathcal{H}_{in}$. Concretely, [15] considers protocols with n qubits of communication and $\mathcal{H}_{in} \cong (\mathbb{C}^2)^{\otimes \nu n}$ for some parameter $\nu > 0$ which we call the *storage rate*. Security of certain protocols was established for $\nu < 1/4$. Furthermore, the protocol proposed by Crépeau [11] for oblivious transfer is secure if the adversary cannot store any quantum information at all, corresponding to a storage rate of $\nu = 0$. Previous work on the noisy-storage model [62] analyzed protocols with n qubits of communication, where the noise $\mathcal{F} \equiv \mathcal{N}^{\otimes n}$ is an n-fold tensor product of a noisy single-qubit channel $\mathcal{N} : \mathcal{B}(\mathbb{C}^2) \to \mathcal{B}(\mathbb{C}^2)$ (i.e., $\mathcal{H}_{in} \cong (\mathbb{C}^2)^{\otimes n}$ and $\nu = 1$). Note, however, that in [62] the adversary was further restricted to performing product measurements on the qubits received in the protocol (albeit otherwise fully arbitrary).

1.4 Main result

We now state our main result of establishing security in the noisy-storage model against *fully general attacks* for arbitrary channels $\mathcal{F} : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$. As explained, we form a very natural relation between the security of our protocols and the problem of transmitting information through the noisy-storage channel[2]. More specifically, we prove that a sufficient condition for security is that the number of classical bits that can be sent through the noisy storage-channel is limited.

As usual in cryptography, we would like to compare the adversary's resources to those of the honest parties and/or the complexity of operations used in the protocol. Here we parametrize these by the number n of qubits transmitted during the protocol. For the adversary's storage, we therefore consider a family $\{\mathcal{F}\}_n$ of storage devices. The quality of the adversary's storage can then be measured (for a fixed n) by the following operational quantity: the success probability of correctly transmitting a randomly chosen nR-bit string $x \in \{0,1\}^{nR}$ through the storage device $\mathcal{F}$, which can be written as

$$P_{succ}^{\mathcal{F}}(nR) := \max_{\{D_x\}_x, \{\rho_x\}_x} \frac{1}{2^{nR}} \sum_{x \in \{0,1\}^{nR}} \mathsf{tr}(D_x \mathcal{F}(\rho_x)) , \tag{2}$$

where the maximum is taken over families of code states $\{\rho_x\}_{x \in \{0,1\}^{nR}}$ on $\mathcal{H}_{in}$ and decoding POVMs $\{D_x\}_{x \in \{0,1\}^{nR}}$ on $\mathcal{H}_{out}$. We show that security can be obtained for arbitrary channels with the property that the decoding probability decays exponentially above a certain threshold:

Theorem 1.1 (Informal statement). *Suppose that for the family of channels $\{\mathcal{F}\}_n$ and the constant $0 < R < 1/2$ there exist constants $n_0 > 0$ and $\gamma > 0$ such that for all $n \geq n_0$ the decoding probability satisfies*

$$P_{\mathrm{succ}}^{\mathcal{F}}(nR) \leq 2^{-\gamma n} . \tag{3}$$

---

[2]The communication problem is equivalent to storing the string, and later trying to read it from the device.

Then oblivious transfer and bit commitment can be implemented using $O(n)$ qubits of communication against an adversary whose noisy storage is described by the family $\{\mathcal{F}\}_n$. Moreover, the security is exponential in n.

Remarkably, the statement of Theorem 1.1 does not require any knowledge of the channel $\mathcal{F}$ beyond its relation to the coding problem. In particular, we do not need to assume that $\mathcal{F}$ is of tensor product form. This includes for example the practically interesting case where errors are likely to occur in bursts in the storage device, or the noisy channel itself has memory. We discuss possible extensions and limitations of our approach in Section 6. We point out that the length of the input strings used in oblivious transfer and bit commitment per communicated qubit depends on the exponent γ in (3); this is hidden in the constant in the O-expression in Theorem 1.1.

Determining the constant γ is of course no easy task for arbitrary storage devices. To obtain explicit security parameters, we thus proceed to consider the special case where the channels are of the form $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$ where n is the number of qubits sent in the protocol, and $\nu \geq 0$ is the *storage rate*. Our proof connects the security of protocols in the noisy-storage model for such channels to the *classical capacity $C_{\mathcal{N}}$* of $\mathcal{N}$. This provides a quantitative expression of our intuition that noisy channels which are of little use for classical information transmission give rise to security in the noisy-storage model. First of all, observe that there can only exist a constant $\gamma > 0$ leading to the exponential decay of (3) if the *classical capacity $C_{\mathcal{N}}$* of the channel is strictly smaller than the rate R at which we send information through the channel. This, however, is not sufficient, since $R > C_{\mathcal{N}}$ is not generally known to imply (3) for $\mathcal{F} = \mathcal{N}^{\otimes n}$. We are therefore interested in channels $\mathcal{N}$ which satisfy the following *strong-converse property*: The success probability (2) decays exponentially for rates R above the capacity, i.e., it takes the form

$$P_{succ}^{\mathcal{N}^{\otimes n}}(nR) \leq 2^{-n\gamma^{\mathcal{N}}(R)} \qquad \text{where} \qquad \gamma^{\mathcal{N}}(R) > 0 \text{ for all } R > C_{\mathcal{N}}. \tag{4}$$

In [36], property (4) was shown to hold for a large class[3] of channels, including the depolarizing channel (see (5) below). It was also shown how to compute $\gamma^{\mathcal{N}}(R)$. Combining Theorem 1.1 with (4), we obtain the following statement:

Corollary 1.2 (Informal statement). *Let $\nu \geq 0$, and suppose that $\mathcal{N}$ satisfies the strong-converse property (4). If*

$$C_{\mathcal{N}} \cdot \nu < \frac{1}{2} \, ,$$

then oblivious transfer and bit commitment can be implemented with polynomial resources (in n) and exponential security against an adversary with noisy storage $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$. For the special case of bounded (noise-free) qubit storage ($C_{\mathcal{N}} = 1$) this gives security for $\nu < 1/2$.

An important example for which we obtain security is the d-dimensional depolarizing channel $\mathcal{N}_r : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ defined for $d \geq 2$ as

$$\mathcal{N}_r(\rho) := r\rho + (1-r)\frac{\mathbb{I}}{d} \qquad \text{for some fixed } 0 \leq r \leq 1 \, , \tag{5}$$

which replaces the input state ρ with the completely mixed state with probability $1 - r$. For $d = 2$, this means that the adversary can store νn qubits, which are affected by independent and identically distributed noise. It has been shown that the depolarizing channel exhibits the strong-converse property [36]. To see for which values of r we can obtain security, we need to consider the classical capacity of the depolarizing channel as evaluated by King [31]. For $d = 2$, i.e., qubits, it is given by

$$C_{\mathcal{N}_r} = 1 + \frac{1+r}{2}\log\frac{1+r}{2} + \frac{1-r}{2}\log\frac{1-r}{2} \, .$$

Figure 1 shows the region in the (r, ν)-plane corresponding to the noise channel $\mathcal{F} = \mathcal{N}_r^{\otimes \nu n}$, where we allow n qubits of communication in the protocol. This is obtained from Corollary 1.2 (The depolarizing channel $\mathcal{N}_r$ satisfies the corresponding conditions).

---

[3]The result of [36] applies to channels with certain covariance properties and additive minimum output α-Rényi entropy. Examples are all unital qubit channels, the Werner-Holevo channel and the depolarizing channel.
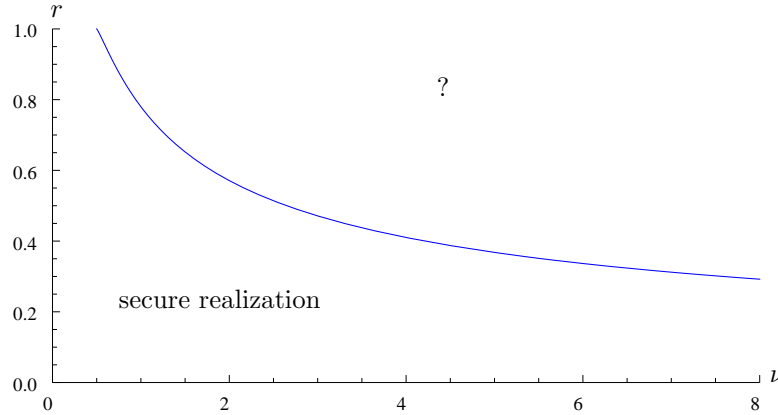
Figure 1: Our results applied to depolarizing noise $\mathcal{F} = \mathcal{N}_r^{\otimes \nu n}$: The vertical axis represents the noise parameter r, while the horizontal axis represents the storage rate ν. Our protocols are secure when the pair (r, ν) is in the lower region bounded by the solid blue curve. Security is still possible in the region labeled with '?', but cannot be obtained from our analysis.

Comparison to the bounded-storage model: depolarizing noise

It was previously observed [53] that the case of depolarizing storage noise (i.e., $r < 1$) can be dealt with using results obtained in the bounded-storage model (i.e., $r = 1$) when the noise is sufficiently strong. More precisely, the results of [15] can be extended to give non-trivial statements if the "effective" dimension of the storage system to be less than $n/4$, where n is the number of qubits communicated in the protocol [4]. We sketch such a simple dimensional analysis to illustrate that our model offers significant improvements over the bounded-storage analysis: we obtain security even at lower noise levels and higher storage rates.
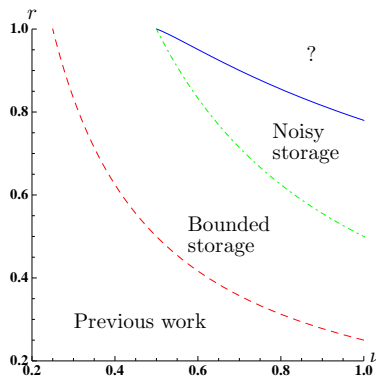
Figure 2: Security for depolarizing noise parameters $(1, \nu)$ with $\nu < 1/4$ was established in the bounded-storage model (BSM). Our simple argument Our more refined protocols and analysis give significantly improved parameters of $\nu < 1/2$ for the bounded-storage model, for which the same argument extends security to the region bounded by the green dot-dashed curve. However, our work still extends this region even further by considering noisy instead of merely bounded storage (solid blue curve). We stress that such a naïve dimensional analysis does not apply to other channels (such as the Two-Pauli channel), while our more refined analysis gives results even in such cases.

Concretely, consider the noise channel $\mathcal{F} = \mathcal{N}_r^{\otimes \nu n} : \mathcal{B}((\mathbb{C}^2)^{\otimes \nu n}) \rightarrow \mathcal{B}((\mathbb{C}^2)^{\otimes \nu n})$ (cf. (5) for $d = 2$).

---

[4]We compare the randomized oblivious transfer protocol of [15] to our protocol based on weak string erasure.

Applying depolarizing noise to any of the νn systems $\mathbb{C}^2$ means that the state on this system is replaced by the completely mixed state with probability $1 - r$. We can think of an indicator random variable $E^{\nu n} = (E_1, \ldots, E_{\nu n}) \in \{0, 1\}^{\nu n}$, where E_i is 1 if and only if the i-th qubit is replaced by the completely mixed state. These "erasure" variables are independent and identically distributed Bernoulli variables with parameter $r = P_{E_i}(0)$. In particular, the number of erasures

$$|E^{\nu n}| = \sum_{i=1}^{\nu n} E_i$$

is distributed according to the binomial distribution with νn trials, each of which succeeds with probability $1 - r$.

We now assume that the adversary is given the location of the erasures $E^{\nu n}$ in addition to the output of the channel. Note that this can only make the adversary more powerful. Conditioned on the locations $E^{\nu n}$, the "effective dimension" of his channel is equal to $2^{\nu n - |E^{\nu n}|}$. Hence, we may think of an "effective" storage rate ν_{eff} given by the random variable

$$\nu_{\text{eff}} = \nu - \frac{|E^{\nu n}|}{n} .$$

We know from the bounded storage model analysis [15] that for $\nu_{\text{eff}} < \frac{1}{4}$, the previously studied protocols provide security. Overall, we therefore conclude that security can be obtained from the noisy channel $\mathcal{F}$ if $\Pr[\nu_{\text{eff}} > \frac{1}{4}]$ is exponentially small. Note that by Chernoff's inequality

$$\Pr[\nu_{\text{eff}} > \frac{1}{4}] = \Pr\left[|E^{\nu n}| < (1 - \delta)\mu\right] < e^{-\mu\delta^2/2} \qquad \text{if } \delta = \frac{1 - 4\nu r}{4\nu(1 - r)} > 0 , \qquad \text{where } \mu = n\nu(1 - r) .$$

In particular, we conclude that we obtain security for

$$\nu r < \frac{1}{4} . \tag{6}$$

Figure 2 compares the curve of this equation (6) to the results we will derive below. We see that for the noiseless case ($r = 1$), our analysis provides security for storage rates $\nu < 1/2$, extending previous results (i.e., $\nu < 1/4$ in [15]) in the bounded-storage model. This improvement stems from the fact that (for oblivious transfer) our protocol uses a different classical post-processing based on interactive hashing instead of the min-entropy splitting tool of [15]. Note that this requires additional rounds of classical communication.

One may wonder whether a security proof may alternatively be obtained based on the idea of simulating the storage noise $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$ using a limited number of qubits. For channels without memory, the quantum reverse Shannon theorem [5] tells us that $\mathcal{F}$ can be simulated using a certain number of (noise-free) qubits when the sender and receiver *share entanglement*. Hence the total size of the system consisting of the noise-free qubits and the entanglement is rather large. However, as explained in [5], the theorem implies an exponential decay of the decoding probability as in (4), but only for rates R greater than the *entanglement-assisted capacity* of the channel $\mathcal{N}$. Our security results thus extend to this regime by our *new* analysis from this paper. Since the latter is greater than the unassisted capacity in general, this suggests that such a simulation-based approach is generally suboptimal: we are essentially overestimating the adversary's capabilities by allowing him to use (noise-free, time-like) entanglement.

Let us give a simple concrete example that provides some intuition on why bounding the adversary's information by the size of his storage device is generally undesirable. Imagine that the adversary's channel $\mathcal{F}$ replaces the n input qubits by a fixed state with overwhelmingly high probability and leaves the input untouched with negligible probability 2^{-n}. Clearly, the number of noise-free qubits required to simulate this channel is equal to n, yet the adversary's decoding probability will be exponentially small. Simply bounding the adversary's information gain in terms of his storage as in the bounded-storage analysis [15] therefore significantly overestimates his abilities.[5]

---

[5]One may argue that this example is artificial, and can easily dealt with by "smoothing": the channel is exponentially close

1.5 Techniques: weak string erasure

Before describing our protocols and proving Theorem 1.1, we give a short overview of the techniques involved.

First, we introduce a primitive called *weak string erasure*, which may be of independent interest. Our protocols for oblivious transfer and bit commitment are then based on this primitive. Weak string erasure provides Alice with a random bit-string $X^n \in \{0,1\}^n$, while Bob receives a randomly chosen substring $X_{\mathcal{I}} = (X_{i_1}, \ldots, X_{i_r})$, together with the index set $\mathcal{I} = \{i_1, \ldots, i_r\}$ specifying the location of these bits. Security of weak string erasure roughly means that Bob will remain ignorant about a significant amount of information about X^n, while security against Alice means that she does not learn anything about $\mathcal{I}$ (for a precise definition, we defer the reader to Section 3).

We provide a protocol for weak string erasure in the noisy-storage model. This protocol can be implemented with present-day hardware used for quantum key distribution. In particular, it does not require the honest parties to have any form of quantum memory. We prove security of this protocol for channels $\mathcal{F}$ as stated in Theorem 1.1. Security against (even an all-powerful) Alice follows from the fact that the protocol only involves one-way communication from Alice to Bob. The security analysis in the presence of a malicious Bob limited by storage noise $\mathcal{F}$ is more involved. Our proof combines an entropic uncertainty relation involving post-measurement information [1, 15] with a reformulation of the problem as a coding scheme: Essentially, the uncertainty relation implies that with high probability (over measurement outcomes), Bob's *classical* information about X^n before using his storage is limited. We then show that this implies that any successful attacker Bob needs to encode classical information at a high rate into his storage device. However, the assumed noisiness of $\mathcal{F}$ precludes this.

Having built a protocol for weak string erasure, we proceed to present protocols for bit commitment and oblivious transfer. The case of bit commitment is particularly appealing: It is essentially only based on weak string erasure and a classical code, and requires little additional analysis. Our approach to realizing oblivious transfer is somewhat more involved: Here weak string erasure is combined with a technique called *interactive hashing* [52]. The output of interactive hashing is a pair of substrings of X, one of which is completely known to Bob, while he only has partial knowledge about the other. Privacy amplification [50] is then used to extract completely random bits. The security analysis of this protocol requires the use of entropy sampling with respect to a a quantum adversary [32].

As as side remark, note that Kilian [29] showed that oblivious transfer is universal for secure two-party computation. In particular, bit commitment could be built from oblivious transfer, but this reduction is generally inefficient.

2 Tools

We briefly introduce all necessary notation as well as several important concepts we will need throughout the paper. For weak string erasure we require the notion of min-entropy (Section 2.2.1), uncertainty relations (Section 2.2.3), as well as an understanding of how storage noise leads to information loss for the cheating party (Section 2.3). In our protocols for bit-commitment and oblivious transfer from weak string erasure, we additionally require the concepts of smooth min-entropy (Section 2.2.2) and secure keys (Section 2.2.4) respectively, and a number of tools, namely privacy amplification (Section 2.4.1), sampling of min-entropy (Section 2.4.2), and finally interactive hashing (Section 2.4.4).

---

to one which can be simulated with no qubits at all. More complex examples exist even classically: Imagine the adversary has some information B about a randomly chosen n-bit classical string X, where B is the result of sending the string X through a classical channel that outputs the first $i \in \{1, \ldots, n\}$ bits of X with probability $p_i = 2^{-i}$ for $i < n$ and $p_i = 2 \cdot 2^{-i}$ for $i = n$. In cryptography the adversary's information is measured in terms of the min-entropy $\mathrm{H}_{\infty}(X|B) = n - \log(1/(n+1))$. Furthermore, $H_0(B) = \log \mathrm{rank}(B) = n$ and for even for a small smoothing parameter $\varepsilon = 2^{-k}$, one still has $H_0^{\varepsilon}(B) \geq n - \log(1/\varepsilon)$. Knowing the size of B only gives us the trivial bound $\mathrm{H}_{\infty}(X|B) \geq \mathrm{H}_{\infty}(X) - H_0(B) = 0$, although the conditional min-entropy is almost maximal.

2.1 Notation

For an integer n, let $[n] := \{1, \ldots, n\}$. We use $2^{[n]} := \{\mathcal{S} \mid \mathcal{S} \subseteq [n]\}$ to refer to the set of all possible subsets of $[n]$, including the empty set $\emptyset$. For an n-tuple $x^n = (x_1, \ldots, x_n) \in \mathcal{X}^n$ over a set $\mathcal{X}$ and a (non-empty) set $\mathcal{I} = \{i_1, \ldots, i_\ell\} \in 2^{[n]}$, we write $x_\mathcal{I}$ for the subtuple $x_\mathcal{I} = (x_{i_1}, \ldots, x_{i_\ell}) \in \mathcal{X}^\ell$.

We use upper case letters to denote a random variable X distributed according to a distribution P_X over a set $\mathcal{X}$, and use lower case letters x for elements $x \in \mathcal{X}$. Joint distributions of e.g., three random variables (X, Y, Z) on $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ are denoted by P_{XYZ}. Given a function $f : \mathcal{X} \to \mathcal{Y}$, any distribution P_X of a random variable X gives rise to another jointly distributed random variable $Y = f(X)$: The joint distribution $P_{XY} \equiv P_{Xf(X)}$ is given by

$$P_{Xf(X)}(x, y) = P_X(x)\delta_{f(x),y} , \tag{7}$$

where $\delta_{i,j}$ is the Kronecker symbol. An important example is the case where $X^n \in \{0,1\}^n$ is a random bitstring and $\mathcal{I} \in 2^{[n]}$ is a random subset of $[n]$, where X^n and $\mathcal{I}$ have joint distribution $P_{X^n\mathcal{I}}$. In this case, the joint distribution $P_{X^n\mathcal{I}Z} \equiv P_{X^n\mathcal{I}X_\mathcal{I}}$ describes e.g., a situation where some bits $Z = X_\mathcal{I}$ of a string X^n are given, together with a specification $\mathcal{I}$ of where these bits are located in the original string.

We use $\mathcal{B}(\mathcal{H})$ to denote the set of bounded operators on a Hilbert space $\mathcal{H}$. A (quantum) *state* is a Hermitian operator $\rho \in \mathcal{B}(\mathcal{H})$ satisfying $\mathrm{tr}(\rho) = 1$ and $\rho \geq 0$. Quantum states can be used to encode classical probability distributions: for a (finite) set $\mathcal{X}$, we fix a Hilbert space $\mathcal{H}_\mathcal{X} \cong (\mathbb{C}^{|\mathcal{X}|})$ and an orthonormal basis $\{|x\rangle \mid x \in \mathcal{X}\}$ of $\mathcal{H}_\mathcal{X}$. This will be referred to as the *computational basis*. A probability distribution P_X on $\mathcal{X}$ can then be encoded into the classical state (*c*-state)

$$\rho_X = \sum_{x \in \mathcal{X}} P_X(x)|x\rangle\langle x| .$$

Of particular interest is the uniform distribution over $\mathcal{X}$, which gives rise to the completely mixed state on $\mathcal{H}_\mathcal{X}$ denoted by the shorthand

$$\tau_\mathcal{X} := \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} |x\rangle\langle x| .$$

States describing classical information (random variables) and truly quantum information simultaneously are termed *classical-quantum* or cq-states. They are described by bipartite systems, where the classical part of the state is diagonal with respect to the computational basis. Concretely, let $\mathcal{H}_Q$ be an additional Hilbert space. A state ρ_{XQ} on $\mathcal{H}_\mathcal{X} \otimes \mathcal{H}_Q$ is a cq-state if it has the form

$$\rho_{XQ} = \sum_{x \in \mathcal{X}} P_X(x)\underbrace{|x\rangle\langle x|}_{X} \otimes \underbrace{\rho_x}_{Q} . \tag{8}$$

In other words, such a state ρ_{XQ} encodes an ensemble of states $\{P_X(x), \rho_x\}_{x \in \mathcal{X}}$ on $\mathcal{H}_Q$, where ρ_x is the *conditional state on Q given $X = x$*. The notion of cq-states directly generalizes to multipartite systems, where classical parts are diagonal with respect to the computational basis. We often fix an ordering of the multipartite parts, and indicate by c or q whether a part is classical or quantum. We can also apply functions to classical parts as before. For a function $f : \mathcal{X} \to \mathcal{Y}$,

$$\rho_{Xf(X)Q} = \sum_{\substack{x \in \mathcal{X}, \\ y \in \mathcal{Y}}} P_{Xf(X)}(x, y)\underbrace{|x\rangle\langle x|}_{X} \otimes \underbrace{|y\rangle\langle y|}_{f(X)} \otimes \underbrace{\rho_x}_{Q} \tag{9}$$

is the ccq-state encoding the pair $(X, f(X))$ of classical random variables (cc) distributed according to (7) as well as the quantum information Q (q) (which depends only on X in this case). Note that in (9), the systems on the rhs. are uniquely determined by the expression on the lhs. We will therefore omit the braces below. Given a state $\rho_{Q_1Q_2}$ on systems Q_1 and Q_2, we also use $\rho_{Q_1} = \mathrm{tr}_{Q_2}(\rho_{Q_1Q_2})$ to denote the state obtained by tracing out Q_2.

The *Hadamard transform* is the unitary described by the matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

in the computational basis $\{|0\rangle, |1\rangle\}$ of the qubit Hilbert space $\mathbb{C}^2$. For the n-qubit Hilbert space, we let

$$H^{\theta^n} |x^n\rangle := H^{\theta_1} |x_1\rangle \otimes \ldots \otimes H^{\theta_n} |x_n\rangle \qquad \text{for } x^n = (x_1, \ldots, x_n), \ \theta^n = (\theta_1, \ldots, \theta_n) \in \{0,1\}^n .$$

We also call states of this form *BB84-states*.

Finally, we need a distance measure for quantum states on a Hilbert space $\mathcal{H}$. We use the distance determined by the trace norm $\|A\|_1 := \mathsf{tr}\sqrt{A^\dagger A}$ for bounded operators $A \in \mathcal{B}(\mathcal{H})$. We will say that two states $\rho, \sigma \in \mathcal{B}(\mathcal{H})$ are *ε-close* if $\frac{1}{2}\|\rho - \sigma\|_1 \leq \varepsilon$, which we also write as

$$\rho \approx_\varepsilon \sigma .$$

2.2 Quantifying adversarial information

2.2.1 Min-entropy and measurements

One of the main properties of the weak string erasure-primitive is that the adversary's (quantum) information Q about the generated bit-string X is limited. To make this statement precise, we first need to introduce an appropriate measure of information. Throughout, we are interested in the case where the adversary holds some (possibly quantum) information Q about a classical random variable X. This situation is described by a cq-state ρ_{XQ} as in (8). A natural measure for the amount of information Q gives about X is the maximal average success probability that a party holding Q has in guessing the value of X. For a given *cq*-state ρ_{XQ}, this *guessing probability* can be written as

$$P_{guess}(X|Q) := \max_{\{D_x\}_x} \sum_x P_X(x)\mathsf{tr}(D_x \rho_x) , \tag{10}$$

where the maximization is over all POVMs $\{D_x\}_{x \in \mathcal{X}}$ on $\mathcal{H}_Q$. It will be convenient to turn (10) into an conditional entropy-like quantity, called the *min-entropy*, which is given by [6]

$$\mathrm{H}_\infty(X|Q) := -\log P_{guess}(X|Q) . \tag{11}$$

Note that the min-entropy was originally defined [49] for arbitrary bipartite states ρ_{AB}, as we will discuss in more detail below.

As an illustrative, yet important, example consider the following ccq-state on $\mathcal{H}_X \otimes \mathcal{H}_\Theta \otimes \mathcal{H}_Q \cong (\mathbb{C}^2)^{\otimes 3}$

$$\rho_{X\Theta Q} = \frac{1}{4} \sum_{x,\theta \in \{0,1\}} |x\rangle\langle x| \otimes |\theta\rangle\langle\theta| \otimes H^\theta |x\rangle\langle x| H^\theta \tag{12}$$

This state arises when encoding a uniformly random bit X using either the computational basis ($\Theta = 0$) or the Hadamard basis ($\Theta = 1$) chosen uniformly at random. Clearly, we have

$$\mathrm{H}_\infty(X) = 1 , \qquad \mathrm{H}_\infty(X|\Theta) = 1 \qquad \text{and} \qquad \mathrm{H}_\infty(X|Q\Theta) = 0 ,$$

where the last identity is a consequence of the fact that given $\Theta = \theta$, the operation H^θ can be undone, such that a subsequent measurement in the computational basis provides X with certainty. Note that this is a special case of the identity

$$\mathrm{H}_\infty(X|Q\Theta) = -\log \mathop{\mathbb{E}}_{\theta \leftarrow P_\Theta} \left[2^{-\mathrm{H}_\infty(X|Q,\Theta=\theta)} \right] , \tag{13}$$

---

[6] All logarithms are taken to base 2.

for a general cq-state $\rho_{XQ\Theta}$ with classical part Θ, where $\mathbb{E}_{\theta \leftarrow P_\Theta}$ denotes the expectation value over the choice of Θ, and $\mathrm{H}_\infty(X|Q, \Theta = \theta)$ is the min-entropy of the conditional state

$$\rho_{X|Q,\Theta=\theta} = \sum_{x \in \{0,1\}} P_{X|\Theta=\theta}(x)|x\rangle\langle x| \otimes H^\theta|x\rangle\langle x|H^\theta \ .$$

Returning to the state (12), it can also be shown [1] that

$$\mathrm{H}_\infty(X|Q) = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \ .$$

2.2.2 Smooth min-entropy

When building oblivious transfer from weak string erasure, we will need to employ a more general definition of the min-entropy given in [49]. For arbitrary (not necessarily unit-trace, or cq) bipartite density operators ρ_{AB} this quantity is defined as

$$\mathrm{H}_\infty(A|B)_\rho = -\log \inf \left\{ \mathsf{tr}(\sigma_B) \mid \sigma_B \geq 0 \text{ and } \rho_{AB} \leq \mathbb{I}_A \otimes \sigma_B \right\} \ , \tag{14}$$

where we use the subscript ρ to indicate what state the quantity refers to. In [34], it was shown via semidefinite programming duality that for a cq-state ρ_{XQ}, definition (14) of $\mathrm{H}_\infty(X|Q)$ coincides with definition (11) in terms of the guessing-probability $P_{guess}(X|Q)$. The advantage of (14) is that it allows us to maximize over neighborhoods of ρ_{XQ}. This leads to the definition of *smooth entropy* [49], which is defined[7] as

$$\mathrm{H}^\varepsilon_\infty(X|Q)_\rho := \sup_{\substack{\bar{\rho}_{XQ} \geq 0 : \frac{1}{2}\|\bar{\rho}_{XQ} - \rho_{XQ}\|_1 \leq \mathsf{tr}(\rho_{XQ})\cdot\varepsilon \\ \mathsf{tr}(\bar{\rho}_{XQ}) \leq \mathsf{tr}(\rho_{XQ})}} \mathrm{H}^\varepsilon_\infty(X|Q)_{\bar{\rho}} \ . \tag{15}$$

We will also use the fact that if ρ_{XQ} is a cq-state, the supremum can be restricted to density operators $\bar{\rho}_{XQ}$ where X is classical and has the same range as the original X. Definition (15) will be convenient for our proof: Roughly, we will construct some state that has high min-entropy. We then show that the state created during a real execution of the protocol is ε-close to this state. By the above definition, the actual state generated in the protocol has high *smooth* min-entropy.

A useful property of the smooth min-entropy is that it obeys a chain rule [49, Theorem 3.2.12], which states that for any *ccq*-state ρ_{XYQ}, we have

$$\mathrm{H}^\varepsilon_\infty(X|YQ)_\rho \geq \mathrm{H}^\varepsilon_\infty(X|Q)_\rho - \log|\mathcal{Y}| \ , \tag{16}$$

where $|\mathcal{Y}|$ is the size of the support of Y.

2.2.3 Uncertainty relations for post-measurement information

When showing the security of weak string erasure, we need to consider a setting where an adversary can first extract some classical information K given access to a quantum system Q and later obtains some additional information Θ. His objective is to guess the value of a random variable X. Suppose he applies a measurement described by a POVM $\{E_k\}_k$ to Q, and retains only the measurement result k. We can think of this as a completely positive trace-preserving map (CPTPM) $\mathcal{K} : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_K)$. When he performs this measurement on the Q-part of a cq-state ρ_{XQ}, we get

$$\rho_{X\mathcal{K}(Q)} := (\mathbb{I}_X \otimes \mathcal{K})(\rho_{XQ}) = \sum_k \mathsf{tr}_Q\left((\mathbb{I}_X \otimes E_k)\rho_{XQ}\right) \otimes |k\rangle\langle k| \ ,$$

---

[7]Unlike in [49], we require that half the 1-norm is bounded. This ensures that $\mathrm{H}^\varepsilon_\infty(X|Q)_\rho \geq \mathrm{H}_\infty(X|Q)_\sigma$ if $\rho_{XQ} \approx_\varepsilon \sigma_{XQ}$.

which is a cc-state (i.e., an encoded joint distribution P_{XK}) if X is classical. Due to its definition, the min-entropy $H_\infty(X|Q)$ is intimately connected with such measurements, and in fact it is easy to see that

$$H_\infty(X|Q) = \min_{\mathcal{K}} H_\infty(X|\mathcal{K}(Q)) .$$ (17)

This important identity relates min-entropies given *quantum* information Q to min-entropies given *classical* information $K = \mathcal{K}(Q)$.

Returning to the example given in (12), let us consider what happens if the adversary learns the basis information Θ *after* the measurement $\mathcal{K}$. In [1, Theorem 4.7] it was shown that the minimal post-measurement min-entropy optimized over all measurements $\mathcal{K}$ obeys

$$\min_{\mathcal{K}} H_\infty(X|\mathcal{K}(Q)\Theta) = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) ,$$

which in the case of our example matches the min-entropy $H_\infty(X|Q)$ without post-measurement information Θ. In our security proof, we will need to consider n repetitions of the state (12), that is,

$$\rho_{X^n\Theta^nQ} = \rho_{X\Theta Q}^{\otimes n} ,$$

where $X^n = (X_1, \ldots, X_n)$ and $\Theta^n = (\Theta_1, \ldots, \Theta_n)$ are n-bit strings, and $\mathcal{H}_Q \cong (\mathbb{C}^2)^{\otimes n}$. It follows from [61, Lemma 2] and [1] that

$$\min_{\mathcal{K}} H_\infty(X^n|\mathcal{K}(Q)\Theta^n) = -n \cdot \log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) .$$ (18)

A generalization of this relation to smooth min-entropy is

$$\min_{\mathcal{K}} H_\infty^\varepsilon(X^n|\mathcal{K}(Q)\Theta^n) \geq n\left(\frac{1}{2} - 2\delta\right) \qquad \text{where } \delta \in]0, \frac{1}{2}[\qquad \text{and}$$ (19)

$$\varepsilon = \exp\left(-\frac{\delta^2 n}{32(2 + \log\frac{1}{\delta})^2}\right) .$$ (20)

This relation follows from [15, Corollary 3.4] using the standard purification trick (cf. [64, Lemma 2.3]). Our construction of a protocol for weak string erasure will make essential use of (18) and (19).

2.2.4 Secure keys and what it means to be ignorant

We will often informally say that an adversary "does not know anything" or "does not learn anything" or "is ignorant" about some random variable X, even when he holds some (quantum) information Q. In terms of the cq-state ρ_{XQ} this means that X is uniformly distributed on $\mathcal{X}$, and independent of Q, that is,

$$\rho_{XQ} = \tau_{\mathcal{X}} \otimes \rho_Q .$$ (21)

Clearly, for such a state, the uncertainty about X given Q is maximal, which in terms of the min-entropy means that $H_\infty(X|Q) = \log|\mathcal{X}|$. For ρ_{XQ} as in (21), X is also referred to as an *ideal key with respect to Q*.

In practice, we are generally forced to work with approximately ideal keys, where X is called a *ε-secure key with respect to Q* if ρ_{XQ} is ε-close to the ideal state $\tau_{\mathcal{X}} \otimes \rho_Q$, that is,

$$\rho_{XQ} \approx_\varepsilon \tau_{\mathcal{X}} \otimes \rho_Q .$$ (22)

This notion of a secure key behaves nicely under composition [3, 50, 33].

2.3 Processes that increase uncertainty

To show the security of weak string erasure, we need to capture the amount of "uncertainty" that an adversary has as a result of his noisy storage $\mathcal{F}$. First, let us consider general processes which increase uncertainty. Note that from the definitions, it is immediate [49, Theorem 3.1.12] that the min-entropy satisfies the following monotonicity property: for every CPTPM $\mathcal{F} : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_{Q'})$, we have

$$H_\infty(X|\mathcal{F}(Q)) \geq H_\infty(X|Q) . \tag{23}$$

An important case is where $\mathcal{H}_Q = \mathcal{H}_{Q_1 Q_2}$ is bipartite, and $\mathcal{F} = \mathsf{tr}_{Q_2}$ is the partial trace over the second system Q_2. We then get

$$H_\infty(X|Q_1) \geq H_\infty(X|Q_1 Q_2) , \tag{24}$$

reflecting the fact that "forgetting" information makes it harder to guess X.

Inequality (23) is insufficient for our purposes, and we will need a more quantitative estimate on the increase of entropy due to a channel $\mathcal{F}$ representing the adversary's memory. Clearly, such an estimate will depend on properties of $\mathcal{F}$. Here we express the bound in terms of the function $P^{\mathcal{F}}_{succ}(n)$ introduced in (2). Intuitively, the following lemma shows that the uncertainty about X after application of $\mathcal{F}$ to Q is related to the problem of transmitting classical bits through the channel $\mathcal{F}$, where the number of bits is given by the min-entropy of X.

Lemma 2.1. *Consider an arbitrary cq-state ρ_{XQ} and a CPTPM $\mathcal{F} : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_{out})$. Then $H_\infty(X|\mathcal{F}(Q)) \geq -\log P^{\mathcal{F}}_{succ}(\lfloor H_\infty(X) \rfloor)$.*

Proof. Let $k := \lfloor H_\infty(X) \rfloor$. It is well-known (see e.g., [56]) that probability distributions P_X with min-entropy at least k are convex combinations of "flat" distributions, i.e., uniform distributions over subsets of $\mathcal{X}$ of size 2^k. In other words, there is a joint distribution P_{XT}, where T is distributed over subsets of size 2^k, such that

$$P_X(x) = \sum_t P_T(t) P_{X|T=t}(x) , \text{ and } P_{X|T=t} \text{ is uniform on } t \subset \mathcal{X} .$$

The distribution P_{XT} together with ρ_{XQ} gives rise to a state ρ_{XQT} whose partial trace is equal to ρ_{XQ}. Again using (24), we get

$$H_\infty(X|\mathcal{F}(Q)) \geq H_\infty(X|\mathcal{F}(Q)T) .$$

By property (13) of the min-entropy when conditioning on classical information, we have

$$H_\infty(X|\mathcal{F}(Q)T) = -\log \mathbb{E}_{t \leftarrow P_T} \left[2^{-H_\infty(X|\mathcal{F}(Q), T=t)} \right] , \tag{25}$$

where $\mathbb{E}_{t \leftarrow P_T}$ denotes the expectation value, and $H_\infty(X|\mathcal{F}(Q), T = t)$ is the min-entropy of the conditional state

$$\rho_{X\mathcal{F}(Q)|T=t} = \sum_x P_{X|T=t}(x)|x\rangle\langle x| \otimes \mathcal{F}(\rho_x) .$$

Now we use the fact that $P_{X|T=t}$ is uniform over a set of size 2^k, and the definition of $P^{\mathcal{F}}_{succ}(n)$. This leads to

$$H_\infty(X|\mathcal{F}(Q), T = t) \geq -\log P^{\mathcal{F}}_{succ}(k) \qquad \text{for all } t \text{ in the support of } P_T . \tag{26}$$

Combining (25) with (26) gives the claim. $\qquad\square$

We now give a straightforward but important generalization of this result.

Lemma 2.2. *Consider an arbitrary ccq-state ρ_{XTQ}, and let $\varepsilon, \varepsilon' \geq 0$ be arbitrary. Let $\mathcal{F} : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_{Q_{out}})$ be an arbitrary CPTPM. Then*

$$\mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X|T\mathcal{F}(Q)) \geq -\log P_{succ}^{\mathcal{F}} \left(\lfloor \mathrm{H}_\infty^\varepsilon(X|T) - \log \frac{1}{\varepsilon'} \rfloor \right) \ .$$

Proof. Clearly, the statement for $\varepsilon = 0$ implies the statement for any $\varepsilon > 0$ because a CPTPM cannot increase distance. To prove the statement for $\varepsilon = 0$, we consider the quantities $2^{-\mathrm{H}_\infty(X|T=t)}$ of the conditional states $\rho_{X|T=t}$, together with the distribution P_T over $\mathcal{T}$ defined by the state ρ_{XTQ}. Applying Markov's inequality $\Pr[Z \geq c] \leq \frac{\mathbb{E}[Z]}{c}$ for any real-valued random variable Z and constant $c > 0$, we obtain

$$\Pr_{t \leftarrow P_T} \left[2^{-\mathrm{H}_\infty(X|T=t)} \geq 2^{-\mathrm{H}_\infty(X|T)+\log\frac{1}{\varepsilon'}} \right] \leq \varepsilon' \left(2^{-\mathrm{H}_\infty(X|T)} \right)^{-1} \mathbb{E}_{t \leftarrow P_T} \left[2^{-\mathrm{H}_\infty(X|T=t)} \right] = \varepsilon' \ .$$

This implies that the distribution P_T has weight at least $1 - \varepsilon'$ on the set

$$\mathcal{G}ood = \left\{ t \in \mathcal{T} \mid \mathrm{H}_\infty(X|T=t) \geq \lfloor \mathrm{H}_\infty(X|T) - \log\frac{1}{\varepsilon'} \rfloor \right\} \ . \tag{27}$$

Accordingly, we can rewrite ρ_{XTQ} as a convex combination

$$\rho_{XTQ} = (1-p) \cdot \rho_{XTQ|T \notin \mathcal{G}ood} + p \cdot \rho_{XTQ|T \in \mathcal{G}ood} \qquad \text{where} \qquad p = P_T(\mathcal{G}ood) \geq 1 - \varepsilon' \ . \tag{28}$$

Set $\sigma_{XTQ} := \rho_{XTQ|T \in \mathcal{G}ood}$. From (28), we conclude that $\frac{1}{2}\|\rho_{XTQ} - \sigma_{XTQ}\|_1 \leq \varepsilon'$. By the monotonicity of the distance under CPTPM, it therefore suffices to show that

$$\mathrm{H}_\infty(X|T\mathcal{F}(Q))_\sigma \geq -\log P_{succ}^{\mathcal{F}} \left(\lfloor \mathrm{H}_\infty(X|T)_\rho - \log\frac{1}{\varepsilon'} \rfloor \right) \ . \tag{29}$$

For this purpose, note that $\sigma_{XT\mathcal{F}(Q)}$ is given by the expression

$$\sigma_{TX\mathcal{F}(Q)} = \sum_{t \in \mathcal{G}ood} P_{T|T \in \mathcal{G}ood}(t) |t\rangle\langle t| \otimes \rho_{X\mathcal{F}(Q)|T=t}$$

In particular, by using (13) again, we have

$$2^{-\mathrm{H}_\infty(X|T\mathcal{F}(Q))_\sigma} = \mathbb{E}_{t \leftarrow P_{T|T \in \mathcal{G}ood}} \left[2^{-\mathrm{H}_\infty(X|\mathcal{F}(Q),T=t)_\rho} \right] \tag{30}$$

Using Lemma 2.1 (applied to the conditional state $\rho_{XQ|T=t}$), we conclude that

$$\mathrm{H}_\infty(X|\mathcal{F}(Q),T=t)_\rho \geq -\log P_{succ}^{\mathcal{F}} \left(\lfloor \mathrm{H}_\infty(X|T)_\rho - \log\frac{1}{\varepsilon'} \rfloor \right) \qquad \text{for all } t \in \mathcal{G}ood \ . \tag{31}$$

The claim (29) immediately follows from (31) and (30). $\qquad\square$

2.4 Defeating a quantum adversary: essential building blocks

In order to build oblivious transfer and bit commitment from weak string erasure, we will employ three additional tools: first, we require *privacy amplification* against a quantum adversary [49, 50] as explained in Section 2.4.1. For oblivious transfer, we also need the notion of *min-entropy sampling* outlined in Section 2.4.2. In particular, we discuss how min-entropy about classical information is approximately preserved when considering randomly chosen subsystems. We then show in Section 2.4.4 how random subsets can be chosen in a cryptographically secure manner with a protocol called *interactive hashing*.

2.4.1 Privacy amplification

Intuitively, privacy amplification allows us to turn a long string X, about which the adversary holds some quantum information Q, into a shorter string $Z = \mathsf{Ext}(X, R)$ about which he is almost entirely ignorant. The maximal length of this new string is directly related to the min-entropy $\mathrm{H}_\infty(X|Q)$ from Section 2.2. In order to obtain this new string, we will need a 2-universal hash function: Formally, a function $\mathsf{Ext} : \{0,1\}^n \otimes \mathcal{R} \to \{0,1\}^\ell$ is called 2-universal if for all $x \neq x' \in \{0,1\}^n$ and uniformly chosen $r \in_R \mathcal{R}$, we have $\Pr[\mathsf{Ext}(x, r) = \mathsf{Ext}(x', r)] \leq 2^{-\ell}$.

Theorem 2.3 (Privacy amplification [49, 50]). *Consider a set of 2-universal hash functions $\mathsf{Ext} : \{0,1\}^n \otimes \mathcal{R} \to \{0,1\}^\ell$, and a cq-state $\rho_{X^n Q}$, where X^n is an n-bit string. Define $\rho_{X^n QR} = \rho_{X^n Q} \otimes \tau_{\mathcal{R}}$, i.e., R is a random variable uniformly distributed on $\mathcal{R}$, and independent of $X^n Q$. Then*

$$\rho_{\mathsf{Ext}(X^n, R)RQ} \approx_{\varepsilon'} \tau_{\{0,1\}^\ell} \otimes \rho_{RQ} \qquad \text{for } \varepsilon' := 2^{-\frac{1}{2}(\mathrm{H}_\infty^\varepsilon(X^n|Q) - \ell) - 1} + 2\varepsilon \qquad \text{for all } \varepsilon > 0 .$$

It is important to stress that the extracted key $\mathsf{Ext}(X^n, R)$ is secure even if the adversary is given R in addition to Q. Theorem 2.3 immediately gives rise to a procedure allowing parties sharing some random variable X^n to extract a key secure against an adversary holding Q. Indeed, one party can simply use independent randomness to pick $r \in_R \mathcal{R}$ uniformly at random, and distribute (publicly) the value of r. Because 2-universal hash functions can be efficiently constructed (e.g., using linear functions [10]), this *privacy amplification protocol* is efficient [9, 27, 7].

2.4.2 Min-entropy sampling with adversarially chosen partitions

For oblivious transfer, we will make use of the sampling property of min-entropy which was first established by Vadhan [59] in the classical case, and in [32] for the classical-quantum case. Consider a cq-state $\rho_{X^n Q}$, where $X^n = (X_1, \ldots X_n)$ is an n-bit string. An important property of smooth min-entropy is that the *min-entropy rate*

$$\frac{\mathrm{H}_\infty^\varepsilon(X^n|Q)}{n} \tag{32}$$

is approximately preserved when considering a randomly chosen substring $X_\mathcal{S}$ of X^n. In some sense, we can therefore think of (32) as the (average) min-entropy of an individual bit X_i given Q.

The corresponding technical statement is slightly more involved. In essence, it requires to pick a subset $\mathcal{S}$ from a distribution $P_\mathcal{S}$ over subsets of $[n]$ with certain properties ($P_\mathcal{S}$ needs to be a so-called *averaging sampler*, see e.g., [22]). For concreteness, we consider the special case where $P_\mathcal{S}$ is uniformly distributed over subsets of size $s = |\mathcal{S}|$. Vadhan's result for the classical case [59] then shows that, for sufficiently large s, we have

$$\frac{\mathrm{H}_\infty^\varepsilon(X_\mathcal{S}|C)}{s} \geq \frac{\mathrm{H}_\infty(X^n|C)}{n} - \delta ,$$

with high probability over the choice of $\mathcal{S}$, for some small $\varepsilon > 0$ and $\delta > 0$. An analogous statement for the cq-case is given in [32]. A major difference is that the result of [32] for the quantum setting requires X_i to be a block, i.e., a β-bit string instead of a single bit.

Since our work is mainly a proof of principle, we do not yet care about optimality or efficiency. We therefore choose $\mathcal{S}$ to be uniform over all subsets of a fixed size s. Furthermore, it is sufficient for our purposes to ensure that the min-entropy rate decreases by at most a factor of 2. This leads to the following statement, which we derive by specializing the results of [32] (see appendix A.1 for details).

Lemma 2.4 (Min-entropy sampling [32]). *Let $\rho_{\mathbf{Z}Q}$ be a cq-state, where $\mathbf{Z} = (Z_{i,\alpha})_{(i,\alpha) \in [m] \times [\beta]} \in \mathbb{M}_{m \times \beta}(\{0,1\})$ is an $m \times \beta$-matrix with entries in $\{0,1\}$. Let $Z_i := (Z_{i,1}, \ldots Z_{i,\beta}) \in \{0,1\}^\beta$ be the i-th row of $\mathbf{Z}$, such that $Z^m = (Z_1, \ldots, Z_m) \equiv \mathbf{Z}$. Let*

$$\frac{\mathrm{H}_\infty^\varepsilon(\mathbf{Z}|Q)}{m\beta} \geq \lambda$$

15

be a lower bound on the smooth min-entropy rate of $\mathbf{Z}$ given Q. Let $\omega \geq 2$ be a constant, and assume $s, \beta \in \mathbb{N}$ are such that

$$s \geq m/4 \qquad and \qquad \beta \geq \max\left\{67, \frac{256\omega^2}{\lambda^2}\right\} , \tag{33}$$

and let $P_{\mathcal{S}}$ be the uniform distributions over subsets of $[m]$ of size s. Then

$$\Pr_{\mathcal{S}}\left[\frac{H_\infty^{\varepsilon+4\delta}(Z_{\mathcal{S}}|Q)}{s\beta} \geq \left(\frac{\omega-1}{\omega}\right)\lambda\right] \geq 1 - \delta^2 \qquad where\ \delta = 2^{-m\lambda^2/(512\omega^2)} .$$

In Lemma 2.4, we have implicitly partitioned βm bits into m blocks $Z_1, \ldots, Z_m$ of β bits each, by arranging the bits in the matrix $\mathbf{Z}$. However, in our protocol we need to extend this result to the case where this partition is chosen arbitrarily, even in an adversarial manner. To formally state the corresponding generalization of Lemma 2.4, first observe that any partition of βm bits into m blocks is described by a permutation $\pi : [m] \times [\beta] \to [m] \times [\beta]$ where $\pi \in S_{m \cdot \beta}$. Given a matrix $\mathbf{Z}$ and a permutation π, let $\pi(\mathbf{Z})_i = (Z_{\pi(i,1)}, \ldots, Z_{\pi(i,\beta)})$ denote the i-th row of the matrix $\pi(\mathbf{Z})$ defined by permuting the entries of $\mathbf{Z}$ using π, and let $\pi(\mathbf{Z})^m = (\pi(\mathbf{Z})_1, \ldots, \pi(\mathbf{Z})_m)$ be the m-tuple of these β-bit rows. We are interested in the min-entropy of the $s\beta$-bit substring $\pi(\mathbf{Z})_{\mathcal{S}} = (\pi(\mathbf{Z})_{i_1}, \ldots, \pi(\mathbf{Z})_{i_s})$, where $\mathcal{S} = \{i_1, \ldots, i_s\} \subset [m]$. Note that the identity permutation $\pi(i, \alpha) = (i, \alpha)$ corresponds to the case of Lemma 2.4.

It will be important that the permutation $\Pi = \pi$ is a random variable which may depend on the adversary's quantum information Q. More precisely, we will assume that Π is the result of a CPTPM applied to Q. Such a CPTPM takes the form $\mathcal{E} : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_{Q'} \otimes \mathcal{H}_\Pi)$, and has the property that Π is classical and a permutation in $S_{m \cdot \beta}$ for any input state. We now generalize Lemma 2.4 to deal with arbitrarily chosen partitions. The generalized version essentially follows from the easily verified fact that the min-entropy is invariant under reordering, i.e.,

$$H_\infty^\varepsilon(\mathbf{Z}|Q) = H_\infty^\varepsilon(\pi(\mathbf{Z})|Q) \qquad for\ all\ permutations \qquad \pi \in S_{m \cdot \beta} . \tag{34}$$

Again, we refer to appendix A.1 for the proof of the following statement.

Lemma 2.5. *Let $\rho_{\mathbf{Z}Q}$ be a cq-state, where $\mathbf{Z} = (Z_{i,\alpha})_{(i,\alpha)\in[m]\times[\beta]} \in \mathbb{M}_{m\times\beta}(\{0,1\})$ is a $m \times \beta$-matrix with entries in $\{0,1\}$. Assume that*

$$\frac{H_\infty^\varepsilon(\mathbf{Z}|Q)}{m\beta} \geq \lambda ,$$

and that λ and $s, \beta \in \mathbb{N}$ satisfy condition (33) of Lemma 2.4. Let $\mathcal{E} : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_{Q'} \otimes \mathcal{H}_\Pi)$ be a permutation-computing CPTPM, as explained above, and let

$$\rho_{\mathbf{Z}Q'\Pi} = (\mathbb{I}_{\mathbf{Z}} \otimes \mathcal{E})\rho_{\mathbf{Z}Q} .$$

Finally, let $P_{\mathcal{S}}$ be the uniform distribution over subsets of $[m]$ of size s. Then for any constant $\omega \geq 2$

$$\Pr_{\mathcal{S}}\left[\frac{H_\infty^{\varepsilon+4\delta}(\Pi(\mathbf{Z})_{\mathcal{S}}|Q'\Pi)}{s\beta} \geq \left(\frac{\omega-1}{\omega}\right)\lambda\right] \geq 1 - \delta^2 \qquad where\ \delta = 2^{-m\lambda^2/(512\omega^2)} .$$

2.4.3 Aborting a protocol

As our protocols allow players to be malicious, they may abort simply by not sending a message. One way to handle this is to add a special symbol "aborted" to the definition of each primitive, and to handle this case separately in the protocol and the proof. For simplicity, we will take a different approach here. Whenever a player does not send any message[8] (or a message that does not have the right format) the other player simply assumes that a particular valid message was sent, for example the string containing only zeros. Obviously, the malicious player could have sent this message himself, so refusing to send a message does not give any advantage to him. From now on we will therefore assume that all players always send a message when they are supposed to.

---

[8]Note that to decide whether Alice has sent a message requires to have an upper bound on the delivery time of a message.

2.4.4 Interactive hashing

A final tool we need is *interactive hashing* [18, 19, 52] first introduced in [47]. This is a two-party primitive where Bob inputs some string W^t, and Alice has no input. The primitive then generates two strings W_0^t, W_1^t, with the property that one of the two equals W^t. For a protocol implementing this primitive, security is intuitively specified by the following conditions: Alice does not learn which of the two strings is indeed equal to W^t. Conversely, Bob should have very little control over the other string created by the protocol. Figure 3 depicts the idealized version of this primitive.
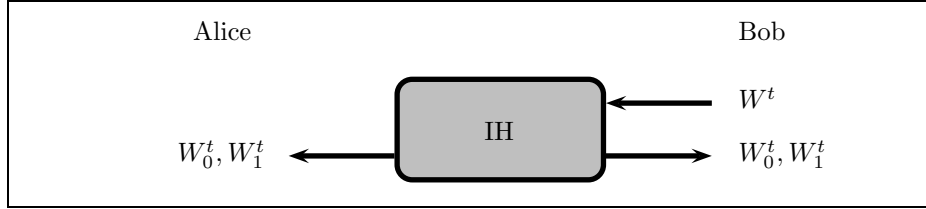

Figure 3: The concept of interactive hashing (IH): Honest Bob has input W^t. Interactive hashing creates substrings W_0^t and W_1^t such that there exists $D \in \{0,1\}$ with $W_D^t = W^t$, where D is unknown to Alice, and Bob has little control over the choice of W_{1-D}^t.

More formally, the following is achieved in [19, Theorem 5.6], where we refer to [52] for the exact parameters used in the security condition for Alice.

Lemma 2.6 (Interactive Hashing [19, 52])**.** *There exists a protocol called* interactive hashing (IH) *between two players, Alice and Bob, where Alice has no input, Bob has input $W^t \in \{0,1\}^t$ and both players output $(W_0^t, W_1^t) \in \{0,1\}^t \times \{0,1\}^t$, satisfying the following:*

Correctness: *If both players are honest, then $W_0^t \neq W_1^t$ and there exists a $D \in \{0,1\}$ such that $W_D^t = W^t$. Furthermore, the distribution of W_{1-D}^t is uniform on $\{0,1\}^t \backslash \{W^t\}$.*

Security for Bob: *If Bob is honest, then $W_0^t \neq W_1^t$ and there exists a $D \in \{0,1\}$ such that $W_D^t = W^t$. If Bob chooses W^t uniformly at random, then D is uniform and independent of Alice's view.*

Security for Alice: *If Alice is honest, then for every subset $\mathcal{S} \subseteq \{0,1\}^t$,*

$$\Pr[W_0^t \in \mathcal{S} \text{ and } W_1^t \in \mathcal{S}] \leq 16 \cdot \frac{|\mathcal{S}|}{2^t}$$

Note that even though this is not explicitly mentioned in [52], aborts need to be treated as explained in Section 2.4.3 to achieve Lemma 2.6.

3 Weak string erasure in the noisy-storage model

We are now ready to introduce our main primitive. After giving a precise security definition in Section 3.1, we present a protocol for realizing this primitive in the noisy-storage model. We will subsequently show that the protocol satisfies the given security definition.

3.1 Definition

"Strong" versus weak string erasure

In an ideal world, string erasure would realize the ideal functionality depicted in Figure 4: It takes no inputs, but provides Alice with a uniformly distributed string n-bit string $X^n = (X_1, \ldots, X_n) \in \{0,1\}^n$, while Bob

receives a random subset $\mathcal{I} = \{i_1, \ldots, i_{|\mathcal{I}|}\} \subset 2^{[n]}$ and the substring $X_\mathcal{I}$. The set of indices $\mathcal{I}$ would thereby be randomly distributed over all the set $2^{[n]}$ of all subsets of $[n]$. Intuitively, we think of the complement of $\mathcal{I}$ as the locations of the "erased" bits.
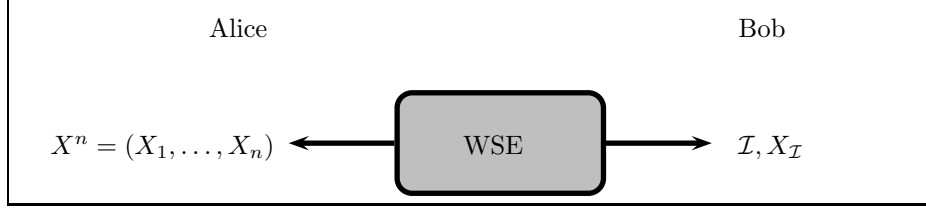

Figure 4: The ideal functionality of string erasure. The actual weak string erasure is somewhat weaker, however, a dishonest party cannot gain significantly more information from the protocol than provided by the "box" depicted above.

Ideally, we would like to realize the functionality in Figure 4 in such a way that even a dishonest party cannot learn anything at all beyond what is provided by the box. Unfortunately, this definition is too stringent to be achieved by our protocol. We therefore relax our functionality to *weak string erasure*, where the players may gain a small amount of additional information. More precisely, we allow a dishonest Bob to learn some information about X^n possibly different from $(\mathcal{I}, X_\mathcal{I})$. However, we demand that his total information about X^n is limited: given a dishonest Bob's system B', he still has some residual amount of uncertainty about X^n. For a dishonest Alice, we essentially retain the strong security property that she does not learn anything about the set of indices $\mathcal{I}$ that Bob receives. In order to obtain bit commitment and oblivious transfer later on, we also demand one additional property that may seem superfluous from a classical perspective, namely that Alice is "committed" to a choice of X^n at the end of the protocol. This difficulty arises since unlike in a classical setting, a dishonest Alice may for example store some quantum information and perform measurements only at a later time. This may allow her to determine parts of X^n after the protocol is completed. Security against such attacks is subtle to define in a quantum setting. To address this problem, we define security in terms of an "ideal" state $\sigma_{A'X^n\mathcal{I}X_\mathcal{I}}$ that could have been obtained by an honest Alice by preparing some state on A' using X^n (i.e., by post-processing). Our security definition then demands that the actual state $\rho_{A'B}$ shared by dishonest Alice and honest Bob after the execution of the protocol has the same form as the partial trace of the ideal state, that is, $\rho_{A'B} = \sigma_{A'\mathcal{I}X_\mathcal{I}}$.

Formal definition

In the following definition of weak string erasure, we write ρ_{AB} for the resulting state at the end of the protocol if both parties are honest, $\rho_{A'B}$ is Alice is dishonest and $\rho_{AB'}$ if Bob is dishonest. Our definition is phrased in terms of ideal states denoted by σ that exhibit all the desired properties of weak string erasure. We then demand that the actual states ρ created during a real execution of the protocol are at least ε-close to such ideal states no matter what kind of attack the dishonest party may perform.

Definition 3.1. *An $(n, \lambda, \varepsilon)$-weak string erasure (WSE) scheme is a protocol between Alice and Bob satisfying the following properties:*

Correctness: *If both parties are honest, then the ideal state $\sigma_{X^n\mathcal{I}X_\mathcal{I}}$ is defined such that*

1. The joint distribution of the n-bit string X^n and subset $\mathcal{I}$ is uniform:

$$\sigma_{X^n\mathcal{I}} = \tau_{\{0,1\}^n} \otimes \tau_{2^{[n]}} \ , \tag{35}$$

2. The joint state ρ_{AB} created by the real protocol is equal to the ideal state:

$$\rho_{AB} = \sigma_{X^n\mathcal{I}X_\mathcal{I}} \ . \tag{36}$$

where we identify (A, B) with $(X^n, \mathcal{I}X_{\mathcal{I}})$.

Security for Alice: *If Alice is honest, then there exists an ideal state $\sigma_{X^n B'}$ such that*

1. *The amount of information B' gives Bob about X^n is limited:*

$$\frac{1}{n}\mathrm{H}_\infty(X^n|B')_\sigma \geq \lambda$$

2. *The joint state $\rho_{AB'}$ created by the real protocol is ε-close to the ideal state:*

$$\sigma_{X^n B'} \approx_\varepsilon \rho_{AB'}$$

where we identify (X^n, B') with (A, B').

Security for Bob: *If Bob is honest, then there exists an ideal state $\sigma_{A'\widehat{X}^n\mathcal{I}}$, where $\widehat{X}^n \in \{0,1\}^n$ and $\mathcal{I} \subseteq [n]$ such that*

1. *The random variable $\mathcal{I}$ is independent of $A'\widehat{X}^n$ and uniformly distributed over $2^{[n]}$:*

$$\sigma_{A'\widehat{X}^n\mathcal{I}} = \sigma_{A'\widehat{X}^n} \otimes \tau_{2^{[n]}} \ .$$

2. *The joint state $\rho_{A'B}$ created by the real protocol condition on the event that Alice does not abort is equal to the ideal state:*

$$\rho_{A'B} = \sigma_{A'(\mathcal{I}\widehat{X}_{\mathcal{I}})}$$

where we identify (A', B) with $(A', \mathcal{I}\widehat{X}_{\mathcal{I}})$.

Note that we do not require X^n to be uniform when Bob is dishonest. To show security of bit commitment and oblivious transfer we will only require that X^n has high min-entropy. The condition that the real state is close to an ideal state having high min-entropy means that the real state has smooth min-entropy as outlined in Section 2.

3.2 Protocol

We now consider a simple protocol achieving weak string erasure in the noisy-storage model using BB84-states. Other encodings are certainly possible, and we will discuss some of the implications of this choice of encoding in Section 6. This protocol is essentially identical to the first step of known protocols for quantum key distribution [65, 4]. However, as explained in the last section, our security requirements differ greatly as we are dealing with two mutually distrustful parties.

Protocol 1: Weak String Erasure (WSE)
Outputs: $x^n \in \{0,1\}^n$ to Alice, $(\mathcal{I}, z^{|\mathcal{I}|}) \in 2^{[n]} \times \{0,1\}^{|\mathcal{I}|}$ to Bob.

1. **Alice:** Chooses a string $x^n \in_R \{0,1\}^n$ and bases-specifying string $\theta^n \in_R \{0,1\}^n$ uniformly at random. She encodes each bit x_i in the basis given by θ_i (i.e., as $H^{\theta_i}|x_i\rangle$) and sends it to Bob.

2. **Bob:** Chooses a basis string $\tilde{\theta}^n \in_R \{0,1\}^n$ uniformly at random. When receiving the i-th qubit, Bob measures it in the basis given by $\tilde{\theta}_i$ to obtain outcome $\tilde{x}_i$.

Both parties wait time Δt.

3. **Alice:** Sends the basis information θ^n to Bob, and outputs x^n.

4. **Bob:** Computes $\mathcal{I} := \{i \in [n] \mid \theta_i = \tilde{\theta}_i\}$, and outputs $(\mathcal{I}, z^{|\mathcal{I}|}) := (\mathcal{I}, \tilde{x}_{\mathcal{I}})$.

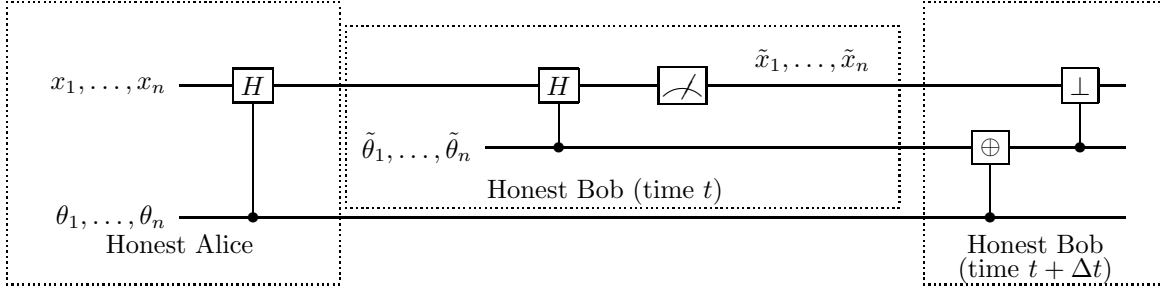---

Our main claim is the following:

Figure 5: The protocol as a circuit. Alice chooses a random string $x^n = (x_1, \ldots, x_n) \in \{0,1\}^n$. She then encodes the bits in random bases specified by $\theta^n = (\theta_1, \ldots, \theta_n) \in \{0,1\}^n$ and sends the corresponding quantum states to Bob. Bob measures in random bases specified by $\tilde{\theta}^n = (\tilde{\theta}_1, \ldots, \tilde{\theta}_n) \in \{0,1\}^n$ obtaining measurement outcomes $\tilde{x}^n = (\tilde{x}_1, \ldots, \tilde{x}_n)$. Upon reception of the basis string θ^n, Bob determines the locations where he measured in the same basis by computing the bit-wise xor $\theta^n \oplus \tilde{\theta}^n = (\theta_1 \oplus \tilde{\theta}_1, \ldots, \theta_n \oplus \tilde{\theta}_n)$. He subsequently discards the bits he measured in the wrong bases (indicated by $\perp$: this replaces the classical input symbol by an erasure symbol).

Theorem 3.2 (Weak string erasure). *(i) Let $\delta \in]0, \frac{1}{2}[$ and let Bob's storage be given by $\mathcal{F} : \mathcal{B}(\mathcal{H}_{\mathrm{in}}) \to \mathcal{B}(\mathcal{H}_{\mathrm{out}})$. Then Protocol 1 is an $(n, \lambda(\delta, n), \varepsilon(\delta, n))$-weak string erasure protocol with min-entropy rate*

$$\lambda(\delta, n) = -\frac{1}{n} \log P_{succ}^{\mathcal{F}} \left(\left(\frac{1}{2} - \delta \right) \cdot n \right) \ ,$$

and error

$$\varepsilon(\delta, n) = 2 \exp \left(-\frac{\delta^2}{512(4 + \log \frac{1}{\delta})^2} \cdot n \right) \ . \tag{37}$$

(ii) Suppose $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$ for a storage rate $\nu > 0$, $\mathcal{N}$ satisfying the strong-converse property (4) and having capacity $C_{\mathcal{N}}$ bounded by

$$C_{\mathcal{N}} \cdot \nu < \frac{1}{2} \ .$$

Let $\delta \in]0, \frac{1}{2} - C_{\mathcal{N}} \cdot \nu[$. Then Protocol 1 is an $(n, \tilde{\lambda}(\delta), \varepsilon(\delta, n))$-weak string erasure protocol for sufficiently large n, where

$$\tilde{\lambda}(\delta) = \nu \cdot \gamma^{\mathcal{N}} \left(\frac{1/2 - \delta}{\nu} \right) \ .$$

It is easy to see that that the protocol is correct if both parties are honest: if Alice is honest, her string $X^n = x^n$ is chosen uniformly at random from $\{0,1\}^n$ as desired, and if Bob is honest, he will clearly obtain $\tilde{x}_i = x_i$ whenever $i \in \mathcal{I}$ for a random subset $\mathcal{I} \subseteq [n]$. The remainder of Section 3 is thus devoted to proving security if one of the parties is dishonest: In Section 3.3, we use the properties of the channel $\mathcal{F}$ to show that the protocol is secure against a dishonest Bob. In Section 3.4, we argue that the protocol satisfies Definition 3.1 when Alice is dishonest.

3.3 Security for honest Alice

We now show that for any cheating strategy of a dishonest Bob, his min-entropy about the string $X^n = (X_1, \ldots, X_n)$ is large. Before turning to the proof, we first explain in Figure 6 how our model restricts the actions of Bob in our protocol. At time t, Bob receives an encoding of a classical string $x^n = (x_1, \ldots, x_n)$
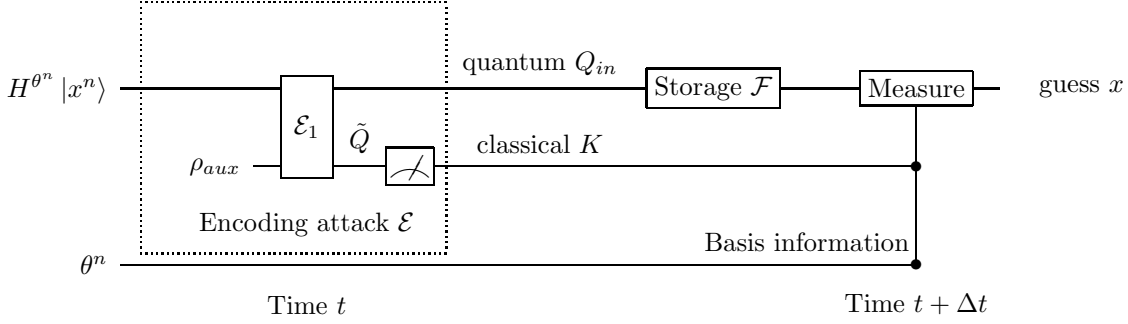
Figure 6: The most general structure of a cheating Bob. Bob's action at time t consists of a CPTPM $\mathcal{E}_1$, followed by a (partial) measurement $\mathcal{K}$, where he may use an arbitrary ancilla ρ_{aux}. At time $t + \Delta t$, Bob can try to reconstruct $x^n = (x_1, \ldots, x_n)$ given the content $\mathcal{F}(Q_{in})$ of the storage device, the classical measurement result $K = \mathcal{K}(\tilde{Q})$, and the basis information $\theta^n = (\theta_1, \ldots, \theta_n)$.

which he would like to reconstruct as accurately as possible. To this end, he can apply any CPTPM $\mathcal{E} : \mathcal{B}((\mathbb{C}^2)^{\otimes n}) \to \mathcal{B}(\mathcal{H}_{in} \otimes \mathcal{H}_K)$ with the following property: For any input state ρ on $(\mathbb{C}^2)^{\otimes n}$, he obtains an output state $\zeta_{Q_{in}K} = \mathcal{E}(\rho)$, where Q_{in} is the quantum information he will put into his quantum storage, and K is any additional classical information he retains. Note that we allow an arbitrary amount of classical storage, that is, $\mathcal{H}_K$ may be arbitrarily large[9]. We call the map $\mathcal{E}$ Bob's *encoding attack*.

We can think of the encoding attack $\mathcal{E}$ as being composed of two steps, $\mathcal{E} = (\mathbb{I}_{Q_{in}} \otimes \mathcal{M}) \circ \mathcal{E}_1$ where Bob first applies an arbitrary CPTPM $\mathcal{E}_1 : \mathcal{B}((\mathbb{C}^2)^{\otimes n}) \to \mathcal{B}(\mathcal{H}_{Q_{in}} \otimes \mathcal{H}_{\tilde{Q}})$, and subsequently performs a measurement $\mathcal{K} : \mathcal{B}(\mathcal{H}_{\tilde{Q}}) \to \mathcal{B}(\mathcal{H}_K)$ on $\mathcal{H}_{\tilde{Q}}$. The outcome of this measurement forms his classical information $K = \mathcal{K}(\tilde{Q})$. For example, Bob can measure some of the incoming qubits, or encode some information using an error-correcting code. The joint state before his storage noise is applied is hence given by

$$\rho_{X^n \Theta^n K Q_{in}} = \frac{1}{(2^n)^2} \sum_{\substack{x^n, \theta^n \in \{0,1\}^n \\ k \in \mathcal{K}}} P_{K|X^n=x^n, \Theta^n=\theta^n}(k) \underbrace{|x^n\rangle\langle x^n| \otimes |\theta^n\rangle\langle\theta^n|}_{\text{Alice}} \otimes \underbrace{|k\rangle\langle k| \otimes \zeta_{x^n \theta^n k}}_{\text{Bob}} , \qquad (38)$$

where $\zeta_{x^n \theta^n k}$ is the conditional state on $\mathcal{H}_{in}$ conditioned on the string $X^n = x^n$, the basis choice $\Theta^n = \theta^n$ and Bob's classical measurement outcome $K = k$. The state (38) is completely determined by Bob's encoding attack $\mathcal{E}$ at time t.

Bob's storage Q_{in} then undergoes noise described by $\mathcal{F} : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$, and the state evolves to $\rho_{X^n \Theta^n K \mathcal{F}(Q_{in})}$. At time $t + \Delta t$, Bob additionally receives the basis information $\Theta^n = \theta^n$. The joint state is now given by

$$\rho_{X^n \Theta^n K \mathcal{F}(Q_{in})} = \frac{1}{(2^n)^2} \sum_{\substack{x^n, \theta^n \in \{0,1\}^n \\ k \in \mathcal{K}}} P_{K|X^n=x^n, \Theta^n=\theta^n}(k) \underbrace{|x^n\rangle\langle x^n|}_{\text{Alice}} \otimes \underbrace{|\theta^n\rangle\langle\theta^n| \otimes |k\rangle\langle k| \otimes \mathcal{F}(\zeta_{x^n \theta^n k})}_{\text{Bob } B'} , \qquad (39)$$

where Bob holds $B' = \Theta^n K \mathcal{F}(Q_{in})$. We now show that Bob's information B' about X^n is limited for large n.

Theorem 3.3 (Security for Alice). *Fix $\delta \in\,]0, \frac{1}{2}[$ and let*

$$\varepsilon = 2\exp\left(-\frac{(\delta/4)^2}{32(2 + \log\frac{4}{\delta})^2} \cdot n\right) .$$

Then for any attack of a dishonest Bob with storage $\mathcal{F} : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$, there exists a cq-state $\sigma_{X^n B'}$ such that

---

[9]It is sufficient for any adversary to store 2^n bits, one for each possible basis string Θ^n [1].

1. $\sigma_{X^n B'} \approx_\varepsilon \rho_{X^n B'}$,

2. $\frac{1}{n} \mathrm{H}_\infty(X^n|B')_\sigma \geq -\frac{1}{n} \log P_{succ}^{\mathcal{F}} \left(\left(\frac{1}{2} - \delta \right) n \right)$,

where $\rho_{X^n B'}$ is given by (39). In particular, if, for some $R < \frac{1}{2}$, we have $\lim_{n \to \infty} -\frac{1}{n} \log P_{succ}^{\mathcal{F}}(nR) > 0$, then $\rho_{X^n B'}$ is exponentially close (in n) to a state $\sigma_{X^n B'}$ with constant min-entropy rate $\frac{1}{n} \mathrm{H}_\infty(X^n|B')_\sigma$.

Proof. We use the notation introduced in (39). By definition (15) of the smooth min-entropy, statements (1) and (2) follow if we show that the smooth min-entropy rate $\frac{1}{n} \mathrm{H}_\infty^\varepsilon(X^n|B')_\rho$ is lower bounded by the expression on the rhs. in (2). By the uncertainty relation (19), we have

$$\mathrm{H}_\infty^{\varepsilon/2}(X^n|\Theta^n K)_\rho \geq \frac{n}{2} - \frac{n\delta}{2} \ .$$

Using Lemma 2.2 applied to $T = (\Theta^n, K)$, we conclude that for $Q_{out} = \mathcal{F}(Q_{in})$ after the noise $\mathcal{F}$ there exists the claimed ideal state and

$$\mathrm{H}_\infty^\varepsilon(X^n|\Theta^n K Q_{out})_\rho \geq -\log P_{succ}^{\mathcal{F}} \left(\frac{n}{2} - \frac{n\delta}{2} - \log \frac{2}{\varepsilon} \right) \geq -\log P_{succ}^{\mathcal{F}} \left(\frac{n}{2} - \frac{n\delta}{2} - \frac{n\delta}{2} \right) \ ,$$

where the final inequality follows from the monotonicity property of the success probability $P_{succ}^{\mathcal{F}}(m) \leq P_{succ}^{\mathcal{F}}(m')$ for $m \geq m'$ and the fact that $\log \frac{2}{\varepsilon} \leq \frac{\delta}{2}n$ because $(\delta/4)^2/(32(2 - \log \delta/4)^2) \leq \delta/2$ for any $0 < \delta < 1/2$. □

Let us specialize Theorem 3.3 to the case where $\mathcal{F}$ is a tensor product channel.

Corollary 3.4. *Let Bob's storage be described by $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$ with $\nu > 0$, where $\mathcal{N}$ satisfies the strong-converse property (4), and*

$$C_\mathcal{N} \cdot \nu < \frac{1}{2} \ .$$

Fix $\delta \in]0, \frac{1}{2} - C_\mathcal{N} \cdot \nu[$, and let $\varepsilon = \varepsilon(\delta, n)$ be defined by (37). Then for any attack of a dishonest Bob, there exists a cq-state $\sigma_{X^n B'}$ such that

1. $\sigma_{X^n B'} \approx_\varepsilon \rho_{X^n B'}$,

2. $\frac{1}{n} \mathrm{H}_\infty(X^n|B')_\sigma \geq \nu \cdot \gamma^\mathcal{N} \left(\frac{1/2 - \delta}{\nu} \right) > 0$,

where $\rho_{X^n B'}$ is given by (39).

Proof. Substituting n by νn and R by R/ν, the strong-converse property (4) turns into

$$-\frac{1}{n} \log P_{succ}^{\mathcal{N}^{\otimes \nu n}}(nR) \geq \nu \cdot \gamma^\mathcal{N}(R/\nu)$$

for sufficiently large n. The claim then follows from Theorem 3.3 by setting $R := \frac{1}{2} - \delta$. □

Theorem 3.3 and Corollary 3.4 establish the first part of Theorem 3.2. It remains to analyze the security against a dishonest Alice.
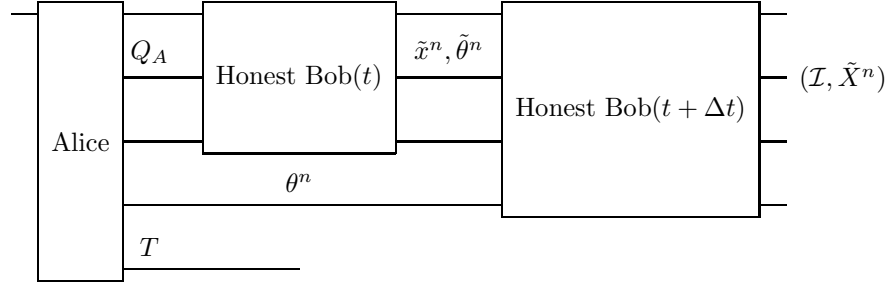
Figure 7: This circuit shows the interaction between a dishonest party Alice and an honest Bob: Alice sends some n-qubit register Q_A and n classical bits θ^n to Bob, and also retains some possibly quantum register T. Honest Bob computes $\mathcal{I}$ and $\tilde{X}^n$ as before. This generates an overall state $\rho_{\Theta^n T \mathcal{I} \tilde{X}^n}$, where Alice's information A' after execution consists of the classical string Θ^n and T.
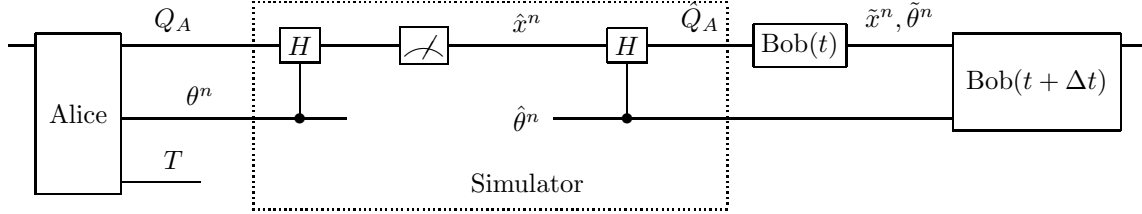

Figure 8: In the security proof, we put an intermediate "simulator" between Alice and Bob to generate the state $\sigma_{A' \hat{X}^n \mathcal{I}}$. We will show the security definition 3.1 is satisfied with $\sigma_{A' \hat{X}^n \mathcal{I}}$. The simulator measures the quantum register in the basis specified by the bit string. He then encodes the measurement result $\hat{X}^n = (\hat{X}_1, \ldots, \hat{X}_n)$ into randomly chosen bases.

3.4 Security for honest Bob

When Alice is dishonest, it is intuitively obvious that she is unable to gain any information about the index set $\mathcal{I}$, since she never receives any information from Bob during our protocol. Yet, in order to obtain bit commitment and oblivious transfer from weak string erasure we require a more careful security analysis. Figure 7 depicts the form of any interaction between a cheating Alice and an honest Bob. Since Alice takes no input in the protocol, her actions are completely specified by the state $\rho_{Q_A \Theta^n T}$ she outputs, where $\mathcal{H}_{Q_A} \cong (\mathbb{C}^2)^{\otimes n}$ is an n-qubit register that she sends to Bob (in the case where Alice is honest, this encodes the string X^n), Θ^n is some classical n-bit string (in the case where Alice is honest, this encodes the bases), and $\mathcal{H}_T$ is an auxiliary register of Alice corresponding to the (quantum) information she holds after execution of the protocol. In the actual protocol, an honest Bob proceeds as shown in Figure 5, that is,

1. Upon receipt of Q_A at time t, an honest Bob measures in randomly chosen bases specified by the string $\tilde{\Theta}^n = (\tilde{\Theta}_1, \ldots, \tilde{\Theta}_n) \in \{0,1\}^n$, obtaining measurement outcomes $\tilde{X}^n = (\tilde{X}_1, \ldots, \tilde{X}_n)$.

2. After receiving $\Theta^n = (\Theta_1, \ldots, \Theta_n)$ at time $t + \Delta t$, he computes the intersecting set $\mathcal{I}$ defined by $\tilde{\Theta}^n$ and Θ^n, and the corresponding substring $\tilde{X}_{\mathcal{I}}$.

The protocol thus creates some state $\rho_{A' \mathcal{I} \tilde{X}_{\mathcal{I}}}$, where $A' = (\Theta^n T)$ is Alice's information, and $B = (\mathcal{I} \tilde{X}_{\mathcal{I}})$ is the information obtained by Bob. Note that this state can be obtained from $\rho_{A' X^n \Theta^n \tilde{\Theta}^n}$ because $\mathcal{I}$ is a function of Θ^n and $\tilde{\Theta}^n$, and $\tilde{X}_{\mathcal{I}}$ is a function of $\tilde{X}^n$ and $\mathcal{I}$.

Theorem 3.5 (Security for Bob)**.** *Protocol 1 satisfies security for honest Bob.*

Proof. We now construct a state $\sigma_{A'\hat{X}^n\mathcal{I}}$ with the required properties. For simplicity, we give an algorithmic description of this state. It is obtained by letting Alice and Bob interact with a simulator which has perfect quantum memory. Note that this simulator is purely imaginary and is merely used to specify the desired ideal state $\sigma_{A'\hat{X}^n\mathcal{I}}$. However, we will later show that the real state created during the protocol equals this ideal state on the registers held by Alice and Bob. Figure 8 summarizes the actions of the simulator:

1. First, the simulator measures the n-qubits Q_A in the bases specified by the bits $\Theta^n = (\Theta_1, \ldots, \Theta_n)$, obtaining measurement outcomes $\hat{X}^n = (\hat{X}_1, \ldots, \hat{X}_n)$.

2. Second, the simulator re-encodes the measurement outcomes $\hat{X}^n$ using randomly chosen bases specified by $\hat{\Theta}^n = (\hat{\Theta}_1, \ldots, \hat{\Theta}_n) \in_R \{0,1\}^n$. He then sends the corresponding qubits to Bob (i.e., the states $H^{\hat{\theta}_i} |\hat{x}_i\rangle$). We call this quantum register $\hat{Q}_A$.

3. Finally, the simulator provides Bob with the basis string $\hat{\Theta}^n = (\hat{\Theta}_1, \ldots, \hat{\Theta}_n)$.

An honest Bob proceeds as before, but with Θ^n replaced by the simulator's string $\hat{\Theta}^n$, and Q_A replaced by the simulator's quantum message $\hat{Q}_A$. As before, Alice's information $A' = (T\Theta^n)$ consists of the string Θ^n and her (quantum) system T. The state $\sigma_{A'\mathcal{I}\tilde{X}_\mathcal{I}}$ held by Alice and Bob can be obtained from $\sigma_{A'\hat{X}^n\hat{\Theta}^n\tilde{\Theta}^n}$, noting that $\hat{X}_\mathcal{I} = \tilde{X}_\mathcal{I}$.

Let us argue that $\sigma_{A'(\mathcal{I}\hat{X}_\mathcal{I})}$ has the properties required by Definition 3.1. First, observe that

$$\sigma_{A'\hat{X}^n\hat{\Theta}^n\tilde{\Theta}^n} = \sigma_{A'\hat{X}^n} \otimes \tau_{\{0,1\}^n} \otimes \tau_{\{0,1\}^n} \ ,$$

since both $\hat{\Theta}^n$ and $\tilde{\Theta}^n$ are chosen uniformly and independently at random by the simulator and Bob, respectively. Since the set $\mathcal{I}$ consists of those indices where $\hat{\Theta}^n$ and $\tilde{\Theta}^n$ agree, we conclude that $\mathcal{I}$ is uniform on the set of subsets of $[n]$, and independent of $A'\hat{\Theta}^n$. That is, the previous identity implies

$$\sigma_{A'\hat{X}^n\mathcal{I}} = \sigma_{A'\hat{X}^n} \otimes \tau_{2^{[n]}} \ , \tag{40}$$

as desired.

It remains to prove that the state created during the real protocol equals this ideal state, that is,

$$\rho_{A'B} = \sigma_{(\Theta^nT)(\mathcal{I}\hat{X}_\mathcal{I})} \ . \tag{41}$$

To produce the state $\sigma_{(\Theta^nT)(\mathcal{I}\hat{X}_\mathcal{I})}$, honest Bob (interacting with the simulator) measures all qubits in the bases $\tilde{\Theta}^n$. Since we are only interested in $\hat{X}_\mathcal{I}$, we could instead apply the first measurement and re-encoding (by the simulator) and the second measurement (by Bob) only on the qubits in $\mathcal{I}$ without affecting the output. But since for all $i \in \mathcal{I}$, we have $\hat{\Theta}_i = \tilde{\Theta}_i$, the re-encoding and the second measurement are always in the same basis, and can therefore be removed. Therefore, the state $\sigma_{\Theta^nT\mathcal{I}\hat{X}_\mathcal{I}}$ can also be produced in the following way: Let Alice output registers (Q_A, Θ^n, T). We first choose $\mathcal{I} \subset [n]$ uniformly at random. Then, we measure all qubits in $\mathcal{I}$ in bases $\Theta_\mathcal{I}$ to get $\hat{X}_\mathcal{I}$, and output registers $(\Theta^n, T, \mathcal{I}, \hat{X}_\mathcal{I})$. Since all qubits in the complement $\mathcal{I}^c$ are discarded anyway, we can measure them in $\tilde{\Theta}_{\mathcal{I}^c}$ without affecting the reduced state $\sigma_{\Theta^nT\mathcal{I}\hat{X}_\mathcal{I}}$. But this exactly what happens in the real protocol producing the state $\rho_{A'B}$, which implies Eq. (41). $\qquad\square$

3.5 Application to concrete tensor product channels

We examine the security parameters we can obtain for several well-known channels. A simple example is the d-dimensional depolarizing channel defined in (5), which replaces the input state ρ with the completely mixed state with probability $1 - r$. Another simple example is the one-qubit two-Pauli channel [30]

$$\mathcal{N}_{\text{Pauli}}(\rho) := r\rho + \frac{1-r}{2}X\rho X + \frac{1-r}{2}Z\rho Z \ .$$

Both these channels obey the strong-converse property (4) (see [36]), allowing us to obtain security of weak string erasure by Corollary 3.4.

For simplicity, we first consider the case where the storage rate is $\nu = 1$, that is, Bob's storage system is $(\mathbb{C}^d)^{\otimes n}$, i.e., n copies of a d-dimensional system, and his noise channel is $\mathcal{F} = \mathcal{N}^{\otimes n}$. We first determine the values of r that allow for a secure implementation of weak string erasure. By Corollary 3.4, the capacity of the channel $\mathcal{N}$ must be bounded by $C_\mathcal{N} < \frac{1}{2}$. The table given in Figure 9 summarizes the relevant parameters.

Channel	Capacity $C_\mathcal{N}$	Reference	Threshold
Qubit depolarizing	$1 + \frac{1+r}{2} \log \frac{1+r}{2} + \frac{1-r}{2} \log \frac{1-r}{2}$	[31]	$r \leq 0.77$
Qutrit depolarizing	$\log 3 + \left(r + \frac{1-r}{3}\right) \log \left(r + \frac{1-r}{3}\right) + 2\frac{1-r}{3} \log \frac{1-r}{3}$	[31]	$r \leq 0.61$
Two-Pauli	$1 - h\left(\frac{1+\max(r, 2r-1)}{2}\right)$	[30]	$r \leq 0.77$

Figure 9: A sufficient condition for achieving security (for storage rate $\nu = 1$) is that the noise parameter r lies below the threshold given above. This is equivalent to $C_\mathcal{N} < \frac{1}{2}$.

When allowing storage rates other than $\nu = 1$, we may again consider the regime where our proof provides security. Figure 10 examines this setting for the qutrit depolarizing channel and the two-Pauli channel, respectively.
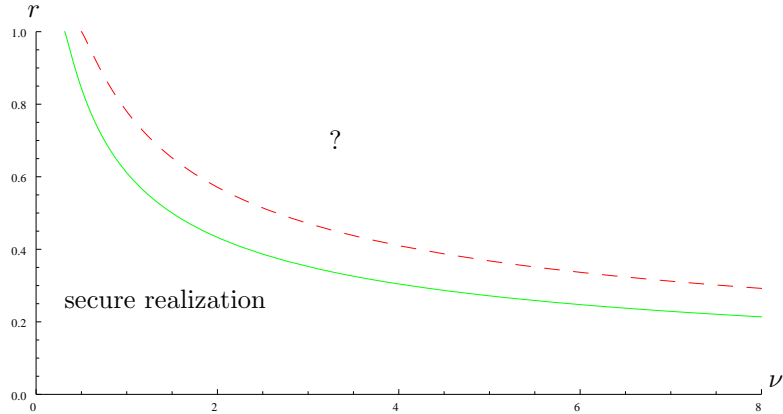

Figure 10: Tradeoff between ν and r: security can be obtained for the qutrit depolarizing channel below solid blue line and the two-Pauli channel below the dashed red line. Note, however, that for the same storage rate the dimension of the storage system is larger for the qutrit than for the qubit channel.

To determine the exact security of the protocol, we need to compute the min-entropy rate

$$\lambda(\delta) = \nu \cdot \gamma^\mathcal{N} \left(\frac{1/2 - \delta}{\nu}\right) ,$$

as stated in Corollary 3.4. For the class of channels $\mathcal{N} : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ considered in [36], the strong converse property (4) was shown to be satisfied with the function $\gamma^\mathcal{N}$ given by

$$\gamma^\mathcal{N}(R) = \max_{\alpha \geq 1} \frac{\alpha - 1}{\alpha} \left(R - \log d + S_\alpha^{\min}(\mathcal{N})\right) ,$$
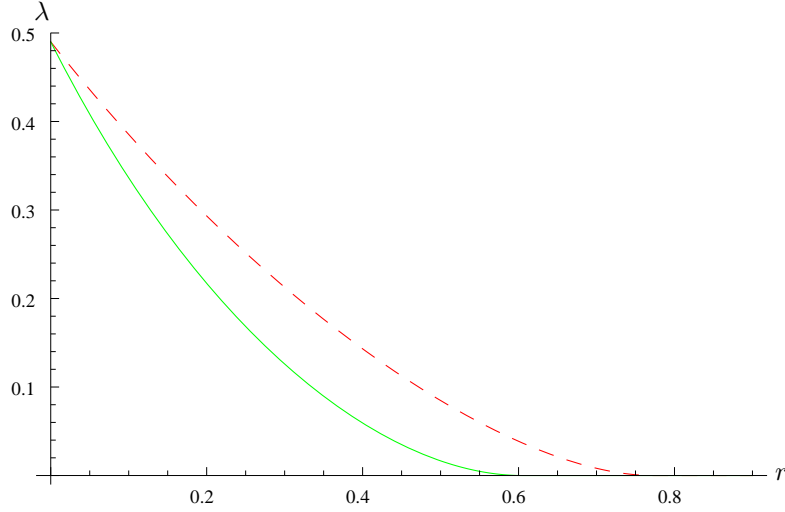
Figure 11: The value of the min-entropy rate λ for the qubit depolarizing channel (dashed red line) and the qutrit depolarizing channel (solid blue line) as a function of the noise parameter r, for $\nu = 1$ and $\delta = 0.01$. Using qutrits means that the dimension of the overall storage system is higher, and we expect the resulting higher capacity to lead to a smaller min-entropy rate λ. Our analysis confirms this intuition.

where $S_\alpha^{\min}(\mathcal{N})$ is the minimum output α-Rényi-entropy of the channel. For the d-dimensional depolarizing channel (see (5)) we may rewrite this expression [31] as

$$
\gamma^{\mathcal{N}}(R) = \max_{\alpha \geq 1} \frac{\alpha - 1}{\alpha} \left(R - \log d + \frac{1}{1-\alpha} \log \left(\left(r + \frac{1-r}{d} \right)^\alpha + (d-1) \left(\frac{1-r}{d} \right)^\alpha \right) \right) \ .
$$

Figure 11 shows how the min-entropy rate $\lambda(\delta)$ relates to the noise parameter r for the qubit and qutrit depolarizing channels for a storage rate of $\nu = 1$ and error $\delta = 0.01$. The figure shows that the min-entropy rate we can achieve in our protocol is directly related to the amount of noise in the storage.

4 Bit commitment from weak string erasure

4.1 Definition

Informally, a standard *commitment scheme* consists of a Commit and an Open primitive between two parties Alice and Bob. First, Alice and Bob execute the Commit primitive, where Alice has input $Y^\ell \in \{0,1\}^\ell$, and Bob has no input. As output, Bob receives a notification that Alice has chosen an input Y^ℓ. Afterwards, they may execute the Open protocol, during which Bob either accepts or rejects. If both parties are honest, Bob always accepts and receives the value Y^ℓ. If Alice is dishonest, however, we still demand that Bob either outputs the correct value of Y^ℓ or rejects (binding). If Bob is dishonest, he should not be able to gain any information about Y^ℓ before the Open protocol is executed (hiding).

Here, we make use of a randomized version of a commitment as depicted in Figure 12. This simplifies both our definition, as well as the protocol. Instead of inputting her own string Y^ℓ, Alice now *receives* a random string C^ℓ from the Commit protocol. Note that if Alice wants to commit to a value Y^ℓ of her choice, she may simply send the xor of her value with the random commitment $Y^\ell \oplus C^\ell$ to Bob at the end of the Commit protocol.

To give a more formal definition, note that we may write the Commit and the Open protocol as CPTPMs $\mathcal{C}_{AB}$ and $\mathcal{O}_{AB}$ respectively, consisting of the local actions of honest Alice and Bob, together with any operations they may perform on messages that are exchanged. When both parties are honest, the output of the Commit protocol will be a state $\mathcal{C}_{AB}(\rho_{\text{in}}) = \rho_{C^\ell UV}$ for some fixed input state ρ_{in}, where $C^\ell \in \{0,1\}^\ell$ is the classical output of Alice, and U and V are the internal states of Alice and Bob respectively. Clearly, if Alice is dishonest, she may not follow the protocol, and we use $\mathcal{C}_{A'B}$ to denote the resulting map. Note
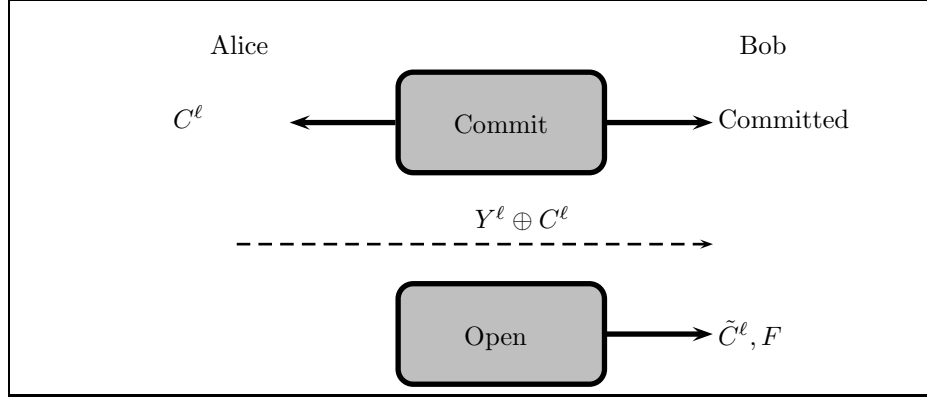
Figure 12: Randomized string commitment: Alice receives a random $C^\ell \in_R \{0,1\}^\ell$ from Commit. During the Open phase, Bob outputs $\tilde{C}^\ell$ and F. If both parties are honest, then $\tilde{C}^\ell = C^\ell$ and $F = accept$. If Alice is dishonest, Bob outputs $F \in \{accept, reject\}$, but $\tilde{C}^\ell = C^\ell$ if $F = accept$. To obtain a standard commitment, Alice can send the extra message indicated by the dashed line.

that $\mathcal{C}_{A'B}$ may not have output C^ℓ, and we hence simply write $\rho_{A'V}$ for the resulting output state, where A' denotes the register of a dishonest Alice. Similarly, we use $\mathcal{C}_{AB'}$ to denote the CPTPM corresponding to the case where Bob is dishonest, and write $\rho_{C^\ell U B'}$ for the resulting output state, where B' denotes the register of a dishonest Bob.

The Open protocol can be described similarly. If both parties are honest, the map $\mathcal{O}_{AB} : \mathcal{B}(\mathcal{H}_{UV}) \to \mathcal{B}(\mathcal{H}_{\tilde{C}^\ell F})$ creates the state $\eta_{C^\ell \tilde{C}^\ell F} := (\mathbb{I}_{C^\ell} \otimes \mathcal{O}_{AB})(\rho_{C^\ell UV})$, where $\tilde{C}^\ell \in \{0,1\}^\ell$ and $F \in \{accept, reject\}$ is the classical output of Bob. Again, if Alice is dishonest, we write $\mathcal{O}_{A'B}$ to denote the resulting CPTPM with output $\eta_{A''\tilde{C}^\ell F}$, and if Bob is dishonest, we write $\mathcal{O}_{AB'}$ for the resulting CPTPM with output $\eta_{C^\ell B''}$. The following definition is similar to the one given in [15], but slightly more general.

Definition 4.1. *An (ℓ, ε)-randomized string commitment scheme is a protocol between Alice and Bob satisfying the following properties:*

Correctness: *If both parties are honest, then the ideal state $\sigma_{C^\ell C^\ell F}$ is defined such that*

1. *The distribution of C^ℓ is uniform, and Bob accepts the commitment:*

$$\sigma_{C^\ell F} = \tau_{\{0,1\}^\ell} \otimes |accept\rangle\langle accept| \ .$$

2. *The joint state $\eta_{C^\ell \tilde{C}^\ell F}$ created by the real protocol is ε-close to the ideal state:*

$$\eta_{C^\ell \tilde{C}^\ell F} \approx_\varepsilon \sigma_{C^\ell C^\ell F} \ ,$$

where we identify (A, B) with $(C^\ell, \tilde{C}^\ell F)$.

Security for Alice (ε-hiding): *If Alice is honest, then for any joint state $\rho_{C^\ell B'}$ created by the Commit protocol, Bob does not learn C^ℓ:*

$$\rho_{C^\ell B'} \approx_\varepsilon \tau_{\{0,1\}^\ell} \otimes \rho_{B'} \ .$$

Security for Bob (ε-binding): *If Bob is honest, then there exists an ideal cqq-state $\sigma_{C^\ell A'V}$ such that for all $\mathcal{O}_{A'B}$:*

1. *Bob almost never accepts $\tilde{C}^\ell \neq C^\ell$:*

For $\psi_{C^\ell A''\tilde{C}^\ell F} = (\mathbb{I}_{C^\ell} \otimes \mathcal{O}_{A'B})(\sigma_{C^\ell A'V}) \ , \ $ we have $\Pr[C^\ell \neq \tilde{C}^\ell \ and \ F = accept] \leq \varepsilon \ .$

2. The joint state $\rho_{A'V}$ created by the real protocol is ε-close to the ideal state:

$$\rho_{A'V} \approx_\varepsilon \sigma_{A'V} \ .$$

4.2 Protocol

Let $\varepsilon' > 0$. To construct our protocol based on weak string erasure, we will need a binary (n, k, d)-linear code $\mathcal{C} \subseteq \{0,1\}^n$, i.e., a linear code with 2^k elements and minimal distance $d := 2\log 1/\varepsilon'$. Let $\mathsf{Syn} : \{0,1\}^n \to \{0,1\}^{n-k}$ be a function that outputs a parity-check syndrome for the code $\mathcal{C}$. Let $\mathsf{Ext} : \{0,1\}^n \times \mathcal{R} \to \{0,1\}^\ell$ be a 2-universal hash function as defined in Section 2.4.1

Protocol 2a: Commit
Inputs: none. Outputs: $c^\ell \in \{0,1\}^\ell$ to Alice.

    1: Alice and Bob: Execute $(n, \lambda, \varepsilon)$-WSE. Alice gets $x^n \in \{0,1\}^n$, and Bob gets $\mathcal{I} \subset [n]$ and $s = x_{\mathcal{I}}$.

    2: Alice: Chooses $r \in_R \mathcal{R}$ and sends r and $w := \mathsf{Syn}(x^n)$ to Bob.

    3: Alice: Outputs $c^\ell := \mathsf{Ext}(x^n, r)$ and stores x^n. Bob stores $(r, w, \mathcal{I}, s)$.

Protocol 2b: Open
Inputs: none. Outputs: $\tilde{c}^\ell \in \{0,1\}^\ell$ and $f \in \{accept, reject\}$ to Bob.

    1: Alice: Sends x^n to Bob.

    2: Bob: If $s \neq x_{\mathcal{I}}$ or $w \neq \mathsf{Syn}(x^n)$, then he outputs $\tilde{c}^\ell := 0^\ell$ and $f := reject$. Otherwise, he outputs $\tilde{c}^\ell := \mathsf{Ext}(x^n, r)$ and $f := accept$.

Our main claim of this section is the following.

Theorem 4.2 (String commitment). *The pair (2a, 2b) of protocols (Commit,Open) is an $(\lambda n - (n-k) - 2\log 1/\varepsilon', 2\varepsilon + \varepsilon')$-randomized string commitment scheme based on one instance of $(n, \lambda, \varepsilon)$-WSE.*

The length $\ell := \lambda n - (n-k) - 2\log 1/\varepsilon'$ of the commitment depends on our choice of code $\mathcal{C}$. Since we require that $\ell > 0$, we need $n - k$ to be small compared to n, which means that we need codes for which $k/n \to 1$ for $n \to \infty$. A simple construction of codes that satisfy this can be based on *Reed-Solomon codes* [48] over the field $GF(2^m)$, which are $(2^m - 1, 2^m - d, d)$-linear codes. We can convert these codes into binary $((2^m - 1)m, (2^m - d)m, d)$-linear codes by simply mapping each field element to m bits. For $n := (2^m - 1)m$, we have $n - k = (d-1)m \leq d(\log n - 1)$, since $n \geq 2 \cdot 2^m$ whenever $m \geq 3$. Therefore, with these codes we can achieve $\ell \geq \lambda n - 2\log n \log 1/\varepsilon$, i.e., our commitment rate is roughly λ.

4.3 Security proof

We again show security for Alice and Bob individually. Recall that if Bob is dishonest, our goal is to show that his information about C^ℓ is negligible. The intuition behind this proof is that weak string erasure ensures that Bob's information about the string X^n is limited. Via privacy amplification we then obtain that his information about C^ℓ, which is the output of a 2-universal hash function applied to X^n, is neglible.

Lemma 4.3 (Security for Alice). *The pair of protocols (Commit,Open) is $(2\varepsilon + \varepsilon')$-hiding.*

Proof. Let $\rho_{X^n B'}$ the cq-state created by the execution of WSE. From the properties of WSE it follows that there exists a state $\sigma_{X^n B'}$ such that $\mathrm{H}_\infty(X^n|B')_\sigma \geq \lambda n$ and $\rho_{X^n B'} \approx_\varepsilon \sigma_{X^n B'}$. This implies that

$$\mathrm{H}_\infty^\varepsilon(X^n|B')_\rho \geq \lambda n \ .$$

By the chain rule (see (16)), we get

$$H^\varepsilon_\infty(X^n|B'\mathsf{Syn}(X^n))_\rho \geq \lambda n - (n-k) = \ell + 2\log 1/\varepsilon' \ .$$

Using privacy amplification (Theorem 2.3), we then get that

$$\frac{1}{2}\|\rho_{C^\ell B'} - \tau_{\{0,1\}^\ell} \otimes \rho_{B'}\|_1 \leq 2\varepsilon + 2^{-\frac{1}{2}\cdot 2\log 1/\varepsilon'-1} \leq 2\varepsilon + \varepsilon' \ ,$$

as promised. □

To show security for honest Bob, we need the following property of linear codes. Note that the function Syn is linear, i.e., for all codewords x^n and $\bar{x}^n$, we have $\mathsf{Syn}(x^n \oplus \bar{x}^n) = \mathsf{Syn}(x^n) \oplus \mathsf{Syn}(\bar{x}^n)$. Therefore, for any x^n and $\bar{x}^n$ with $x^n \neq \bar{x}^n$ and $\mathsf{Syn}(x^n) = \mathsf{Syn}(\bar{x}^n)$, we have that the string $\mathsf{Syn}(x^n \oplus \bar{x}^n) \in \{0,1\}^{n-k}$ is the all zero string 0^{n-k}. From this it follows that $x^n \oplus \bar{x}^n$ is a codeword different from 0^n. Since all codewords except 0^n have weight at least d, it follows that x^n and $\bar{x}^n$ have distance at least d.

The intuition behind the following proof is the observation that weak string erasures ensures that Bob knows the substring $\hat{X}_\mathcal{I}$ of a string $\hat{X}$. The properties of the error-correcting code limit the set of strings X^n consistent with this substring and the given syndrome W; this implies that Alice will be detected with high probability if she attempts to cheat.

Lemma 4.4 (Security for Bob). *The pair of protocols (Commit,Open) is ε-binding.*

Proof. Let $\rho_{A'B}$ be the state shared by Alice and Bob after the execution of WSE. From the properties of WSE it follows that there exists a state $\sigma_{A'\hat{X}^n\mathcal{I}} = \sigma_{A'\hat{X}^n} \otimes \tau_{2^{[n]}}$ such that $\rho_{A'B} = \sigma_{A'(\mathcal{I}\hat{X}_\mathcal{I})}$, where $B = (\mathcal{I}\hat{X}_\mathcal{I})$. Let $\bar{X}^n$ be the closest string to $\hat{X}^n$ that satisfies $\mathsf{Syn}(\bar{X}^n) = W$, and let $C^\ell := \mathsf{Ext}(\bar{X}^n, R)$. We will now show that the state $\sigma_{C^\ell A'(RW\mathcal{I}S)}$ created during the Commit protocol satisfies the binding condition.

First of all, note that if Alice sends $X^n = \bar{X}^n$, then Bob outputs $\tilde{C}^\ell = C^\ell$. It thus remains to analyze the case of $X^n \neq \bar{X}^n$. Note that we may write

$$\Pr[C^\ell \neq \tilde{C}^\ell \text{ and } F = accept]$$

$$= \Pr_{\substack{R,X^n,\bar{X}^n \\ \mathsf{Syn}(X^n)\neq\mathsf{Syn}(\bar{X}^n)}} [\mathsf{Ext}(\bar{X}^n, R) \neq \mathsf{Ext}(X^n, R) \text{ and } F = accept]$$

$$+ \Pr_{\substack{R,X^n,\bar{X}^n \\ \mathsf{Syn}(X^n)=\mathsf{Syn}(\bar{X}^n)}} [\mathsf{Ext}(\bar{X}^n, R) \neq \mathsf{Ext}(X^n, R) \text{ and } F = accept]$$

$$= \Pr_{\substack{R,X^n,\bar{X}^n \\ \mathsf{Syn}(X^n)=\mathsf{Syn}(\bar{X}^n)}} [\mathsf{Ext}(\bar{X}^n, R) \neq \mathsf{Ext}(X^n, R) \text{ and } F = accept]$$

where the last equality follows from the fact that Bob always rejects if $\mathsf{Syn}(X^n) \neq \mathsf{Syn}(\bar{X}^n)$.

We now show that the remaining term is small. Note that if $\mathsf{Syn}(X^n) = \mathsf{Syn}(\bar{X}^n)$, and $X^n \neq \bar{X}^n$, the distance between X^n and $\bar{X}^n$ is at least d. We also know that for our choice of $\bar{X}^n$, the distance between $\bar{X}^n$ and $\hat{X}^n$ is at most $d/2$. Hence, X^n has distance at least $d/2$ to $\hat{X}^n$. Since Alice does not know $\mathcal{I}$ and every $i \in [n]$ is in $\mathcal{I}$ with probability $\frac{1}{2}$, Bob accepts with probability at most $\varepsilon = 2^{-d/2}$. Hence, we obtain

$$\Pr[C^\ell \neq \tilde{C}^\ell \text{ and } F = accept] \leq \varepsilon' \ ,$$

as promised. □

It remains to show that the protocol is correct. This follows essentially from the properties of weak string erasure. However, we still need to demonstrate that the state we obtain from weak string erasure has C^ℓ close to uniform.

Lemma 4.5 (Correctness)**.** *The pair of protocols (Commit,Open) satisfies correctness with an error of at most $2\varepsilon + \varepsilon'$.*

Proof. Let $\eta_{C^\ell \tilde{C}^\ell}$ be the state at the end of the protocol. It follows directly from the properties of WSE that $\eta_{C^\ell \tilde{C}^\ell} = \eta_{C^\ell C^\ell}$. It remains to show that this state is close to the ideal state $\sigma_{C^\ell C^\ell}$. By the same arguments as in Lemma 4.3 it follows that $\frac{1}{2}\|\eta_{C^\ell} - \sigma_{C^\ell}\|_1 \le 2\varepsilon + \varepsilon'$. Hence, we also have $\frac{1}{2}\|\eta_{C^\ell C^\ell} - \sigma_{C^\ell C^\ell}\|_1 \le 2\varepsilon + \varepsilon'$. $\qquad\square$

5   1-2 oblivious transfer from weak string erasure

5.1   Definition

We now show how to obtain 1-2 oblivious transfer given access to weak string erasure. Usually, one considers a non-randomized version of 1-2 oblivious transfer, in which Alice has two inputs $Y_0^\ell, Y_1^\ell \in \{0,1\}^\ell$, and Bob has as input a choice bit $D \in \{0,1\}$. At the end of the protocol Bob receives Y_D^ℓ, and Alice receives no output. The protocol is considered secure if the parties do not gain any information beyond this specification, that is, Alice does not learn D and there exists some input Y_{1-D}^ℓ about which Bob remains ignorant.

Here, we again make use of fully randomized oblivious transfer. Fully randomized oblivious transfer takes no inputs, and outputs two strings $S_0^\ell, S_1^\ell \in \{0,1\}^\ell$ to Alice, and a choice bit $C \in \{0,1\}$ and S_C^ℓ to Bob. Security means that if Alice is dishonest, she should not learn anything about C. Similar to weak string erasure, we also demand that two strings S_0^ℓ and S_1^ℓ are created by the protocol. Intuitively, this ensures that just like in a classical protocol, we can again think of the protocol as being completed once Alice and Bob have exchanged their final message. If Bob is dishonest, we demand that there exists some random variable C such that Bob is entirely ignorant about S_{1-C}^ℓ. That is, he may learn at most one of the two strings which are generated.

Fully randomized oblivious transfer can easily be converted into "standard" oblivious transfer as depicted in Figure 13 using the protocol presented in [8] (see also [2]). To obtain non-randomized 1-2 oblivious transfer, Bob sends Alice a message indicating whether $C = D$. Note that since Alice does not know C, she also does not know anything about D. If $C = D$, Alice sends Bob $Y_0^\ell \oplus S_0^\ell$, and $Y_1^\ell \oplus S_1^\ell$, otherwise she sends $Y_0^\ell \oplus S_1^\ell$ and $Y_1^\ell \oplus S_0^\ell$. Clearly, if Bob does not learn anything about S_{1-C}^ℓ, he can learn at most one of Y_0^ℓ and Y_1^ℓ [8, 2].
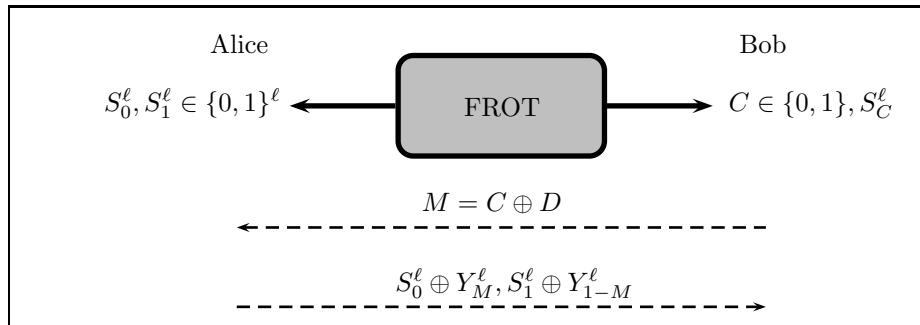
Figure 13: Fully randomized 1-2-oblivious transfer when Alice and Bob are honest. Intuitively, if one of the parties is dishonest, he/she should not be able to obtain more information from the primitive as depicted above. The dashed messages are exchanged to obtain non-randomized oblivious transfer from FROT.

We now provide a more formal definition, which is very similar to the definitions in [15, 21].

Definition 5.1. *An (ℓ, ε)-fully randomized oblivious transfer (FROT) scheme is a protocol between Alice and Bob satisfying the following:*

Correctness: *If both parties are honest, then the ideal state $\sigma_{S_0^\ell S_1^\ell C S_C^\ell}$ is defined such that*

1. The distribution over S_0^ℓ, S_1^ℓ and C is uniform:

$$\sigma_{S_0^\ell S_1^\ell C} = \tau_{\{0,1\}^\ell} \otimes \tau_{\{0,1\}^\ell} \otimes \tau_{\{0,1\}} \ .$$

2. The real state $\rho_{S_0^\ell S_1^\ell C Y^\ell}$ created during the protocol is ε-close to the ideal state:

$$\rho_{S_0^\ell S_1^\ell C Y^\ell} \approx_\varepsilon \sigma_{S_0^\ell S_1^\ell C S_C^\ell} \ , \tag{42}$$

where we identify $A = (S_0^\ell, S_1^\ell)$ and $B = (C, Y^\ell)$.

Security for Alice: *If Alice is honest, then there exists an ideal state* $\sigma_{S_0^\ell S_1^\ell B' C}$, *where C is a random variable on $\{0,1\}$, such that*

1. Bob is ignorant about S_{1-C}^ℓ:

$$\sigma_{S_{1-C}^\ell S_C^\ell B' C} \approx_\varepsilon \tau_{\{0,1\}^\ell} \otimes \sigma_{S_C^\ell B' C} \ .$$

2. The real state $\rho_{S_0^\ell S_1^\ell B'}$ created during the protocol is ε-close to the ideal state:

$$\rho_{S_0^\ell S_1^\ell B'} \approx_\varepsilon \sigma_{S_0^\ell S_1^\ell B'} \ .$$

Security for Bob: *If Bob is honest, then there exists an ideal state* $\sigma_{A' S_0^\ell S_1^\ell C}$ *such that*

1. Alice is ignorant about C:

$$\sigma_{A' S_0^\ell S_1^\ell C} = \sigma_{A' S_0^\ell S_1^\ell} \otimes \tau_{\{0,1\}} \ .$$

2. The real state $\rho_{A' C Y^\ell}$ created during the protocol is ε-close to the ideal state:

$$\rho_{A' C Y^\ell} \approx_\varepsilon \sigma_{A' C S_C^\ell} \ ,$$

where we identify $B = (C, Y^\ell)$.

Again, we allow the protocol implementing this primitive to abort, but demand that the security conditions are satisfied if the protocol does not abort.

5.2 Protocol

We now show how to obtain a fully randomized oblivious transfer given access to weak string erasure.

As in Section 3, honest players never abort the protocol. If the dishonest player refuses to send correctly formed messages, the honest player chooses the messages himself. Note that we require the same also from the interactive hashing protocol: The one player aborts it, the other terminates the protocol. Indeed, this is needed to really satisfy Lemma 2.6, which does not deal with aborts. By inspection of the protocols, it is easy to see that the honest player can indeed simulate all the other players messages in this way.

To obtain some intuition for the actual protocol, consider the following naïve protocol, which we only state informally. It makes use of a 2-universal hash function $\mathsf{Ext} : \{0,1\}^{n/4} \times \mathcal{R} \to \{0,1\}^\ell$.

> **Protocol 3': Naïve Protocol (informal)**
> Outputs: $(s_0^\ell, s_1^\ell) \in \{0,1\}^\ell \times \{0,1\}^\ell$ to Alice, and $(c, y^\ell) \in \{0,1\} \times \{0,1\}^\ell$ to Bob
>
> **1: Alice and Bob:** Execute WSE. Alice gets a string $x^n \in \{0,1\}^n$, Bob a set $\mathcal{I} \subset [n]$ and a string $s = x_\mathcal{I}$. If $|\mathcal{I}| < n/4$, Bob randomly adds elements to $\mathcal{I}$ and pads the corresponding positions in s with 0s. Otherwise, he randomly truncates $\mathcal{I}$ to size $n/4$, and deletes the corresponding values in s.
>
> **2: Alice and Bob:** Execute interactive hashing with Bob's input w equal to a description of $\mathcal{I} = \mathsf{Enc}(w)$. Interpret the outputs w_0 and w_1 as descriptions of subsets $\mathcal{I}_0$ and $\mathcal{I}_1$ of $[n]$.
>
> **3: Alice:** Chooses $r_0, r_1 \in_R \mathcal{R}$ and sends them to Bob.
>
> **4: Alice:** Outputs $(s_0^\ell, s_1^\ell) := (\mathsf{Ext}(x_{\mathcal{I}_0}, r_0), \mathsf{Ext}(x_{\mathcal{I}_1}, r_1))$.
>
> **5: Bob:** Computes $c \in \{0,1\}$ with $\mathcal{I} = \mathcal{I}_c$, and $x_\mathcal{I}$ from s. He outputs $(c, y^\ell) := (c, \mathsf{Ext}(s, r_c))$.

For now, let us neglect the fact that the outputs of interactive hashing are strings, and assume that the subset $\mathcal{I}_{1-c}$ generated by the interactive hashing protocol is uniformly distributed over subsets of size $n/4$ not equal to $\mathcal{I}$. The string $x_{\mathcal{I}_{1-c}}$ is then obtained by sampling from the string x^n, which by the definition of weak string erasure has high min-entropy. We therefore expect the value s_{1-c}^ℓ to be uniform and independent of Bob's view. This should imply security for Alice, whereas security for Bob immediately follows from the properties of interactive hashing.

In this intuitive argument, we have ignored the fact that the sampling result only applies to blocks, and not individual bits. To make use of the sampling results we hence need to make slight modification to the simple protocol given above. We partition x^n (where $n = \beta m$) into m blocks of β bits each. It will be convenient to arrange the bits of x^n into a matrix $\mathbf{z} \in \mathbb{M}_{m \times \beta}(\{0,1\})$, where $\mathbf{z}_{j,\alpha} := x_{(j-1)\cdot\beta+\alpha}$. Note, however, that we cannot simply sample from the rows of $\mathbf{z}$, since the subset $\mathcal{I}$ of bits known to Bob does not correspond to the union of certain rows. We therefore allow Bob to permute the entries of $\mathbf{z}$ by picking a permutation $\pi : [m] \times [\beta] \to [m] \times [\beta]$ such that he knows a subset $\mathcal{J} \subset [m]$ of $|\mathcal{J}| = m/4$ rows of $\pi(\mathbf{z})$. More formally,

$$\exists \mathcal{J} \subset [m], |\mathcal{J}| = m/4 : \text{ if } j' \in \mathcal{J}, \alpha' \in [m] \text{ then } (j-1) \cdot \beta + \alpha \in \mathcal{I} \text{ with } (j, \alpha) = \pi^{-1}(j', \alpha') . \tag{43}$$

Bob announces the permutation π to Alice, and both parties continue to use $\pi(\mathbf{z})$ instead of $\mathbf{z}$. It turns out that picking π at random subject to (43) ensures that Bob's input $\mathcal{J}$ to the interactive hashing protocol does not reveal any significant information about c to Alice. This will be shown below.

To use interactive hashing in conjunction with subsets, the actual protocol needs an encoding of subsets $\mathsf{Enc} : \{0,1\}^t \to \mathcal{T}$, where $\mathcal{T}$ is the set of all subsets of $[m]$ of size $m/4$ (we assume without loss of generality that m is a multiple of 4). Here we choose t such that $2^t \leq \binom{m}{m/4} \leq 2 \cdot 2^t$, and an injective encoding $\mathsf{Enc} : \{0,1\}^t \to \mathcal{T}$, i.e., no two strings are mapped to the same subset. Note that this means that not all possible subsets are encoded, but at least half of them. We refer to [19, 52] for details on how to obtain such an encoding.

Protocol 3: WSE-to-FROT

Parameters: Integers n, β such that $m := n/\beta$ is a multiple of 4. Set $t := m/2$. Outputs: $(s_0^\ell, s_1^\ell) \in \{0,1\}^\ell \times \{0,1\}^\ell$ to Alice, and $(c, y^\ell) \in \{0,1\} \times \{0,1\}^\ell$ to Bob

  1: Alice and Bob: Execute $(n, \lambda, \varepsilon)$-WSE. Alice gets a string $x^n \in \{0,1\}^n$, Bob a set $\mathcal{I} \subset [n]$ and a string $s = x_\mathcal{I}$. If $|\mathcal{I}| < n/4$, Bob randomly adds elements to $\mathcal{I}$ and pads the corresponding positions in s with 0s. Otherwise, he randomly truncates $\mathcal{I}$ to the size $n/4$, and deletes the corresponding values in s.

      We arrange x^n into a matrix $\mathbf{z} \in \mathbb{M}_{m \times \beta}(\{0,1\})$, by $\mathbf{z}_{j,\alpha} := x_{(j-1)\cdot\beta+\alpha}$ for $(j, \alpha) \in [m] \times [\beta]$.

  2: Bob:

    1. Randomly chooses a string $w^t \in_R \{0,1\}^t$ corresponding to an encoding of a subset $\mathsf{Enc}(w^t)$ of $[m]$ with $m/4$ elements.

    2. Randomly partitions the n bits of x^n into m blocks of β bits each: He randomly chooses a permutation $\pi : [m] \times [\beta] \to [m] \times [\beta]$ of the entries of $\mathbf{z}$ as in Lemma 2.5, such that he knows $\pi(\mathbf{z})_{\mathsf{Enc}(w^t)}$ (that is, these bits are permutation of the bits of s). Formally, π is uniform over permutations satisfying the following condition: for all $(j, \alpha) \in [m] \times [\beta]$ and $(j', \alpha') := \pi(j, \alpha)$, we have $(j-1) \cdot \beta + \alpha \in \mathcal{I} \Leftrightarrow j' \in \mathsf{Enc}(w^t)$.

    3. Bob sends π to Alice.

  3: Alice and Bob: Execute interactive hashing with Bob's input equal to w^t. They obtain $w_0^t, w_1^t \in \{0,1\}^t$ with $w^t \in \{w_0^t, w_1^t\}$.

  4: Alice: Chooses $r_0, r_1 \in_R \mathcal{R}$ and sends them to Bob.

  5: Alice: Outputs $(s_0^\ell, s_1^\ell) := (\mathsf{Ext}(\pi(\mathbf{z})_{\mathsf{Enc}(w_0^t)}, r_0), \mathsf{Ext}(\pi(\mathbf{z})_{\mathsf{Enc}(w_1^t)}, r_1))$.

  6: Bob: Computes c, where $w^t = w_c^t$, and $\pi(\mathbf{z})_{\mathsf{Enc}(w^t)}$ from s. He outputs $(c, y^\ell) := (c, \mathsf{Ext}(\pi(\mathbf{z})_{\mathsf{Enc}(w^t)}, r_c))$.

Theorem 5.2 (Oblivious transfer). *For any constant $\omega \geq 2$ and $\beta \geq \max\{67, 256\omega^2/\lambda^2\}$, the protocol WSE-to-FROT implements an $(\ell, 41 \cdot 2^{-\frac{\lambda^2}{512\omega^2\beta}n} + 2\varepsilon)$-FROT from one instance of of $(n, \lambda, \varepsilon)$-WSE, where $\ell := \left\lfloor \left(\left(\frac{\omega-1}{\omega}\right)\frac{\lambda}{8} - \frac{\lambda^2}{512\omega^2\beta}\right)n - \frac{1}{2} \right\rfloor$.*

Since this work is a proof of principle, we may choose $\omega = 2$. However, if we were to look at a more practical setting, choosing other values of ω can be beneficial.

5.3 Security proof

We first show that the protocol is secure against a cheating Alice. Intuitively, the properties of weak string erasure ensure that Alice does not know which bits $x_\mathcal{I}$ of x^n are known to Bob, that is, she is ignorant about the index set $\mathcal{I}$. This implies that essentially any partition of the bits is consistent with Alice's view. In particular, she does not gain much information from the particular partition chosen by Bob. Finally, the properties of interactive hashing ensure that she cannot gain much information about which of the two final strings is known to Bob.

Lemma 5.3 (Security for Bob). *Protocol WSE-to-FROT satisfies security for Bob.*

Proof. Let $\tilde{\rho}_{A''CY^\ell}$ denote the joint state at the end of the protocol, where A'' is the quantum output of a malicious Alice and (C, Y^ℓ) is the classical output of an honest Bob. We construct an ideal state $\tilde{\sigma}_{A''W_0^\ell W_1^\ell C} = \tilde{\sigma}_{A''W_0^\ell W_1^\ell} \otimes \tau_{\{0,1\}}$ that satisfies $\tilde{\rho}_{A''CY^\ell} = \tilde{\sigma}_{A''CW_C^\ell}$.

First, we divide a malicious Alice into two parts. The first part interacts with Bob in the WSE protocol, after which the state shared by Alice and Bob is $\rho_{A'X_{\mathcal{I}}\mathcal{I}}$. From the properties of WSE it follows that there exists an ideal state $\sigma_{A'\hat{X}^n\mathcal{I}\hat{X}_{\mathcal{I}}}$ such that the reduced state satisfies $\rho_{A'X_{\mathcal{I}}\mathcal{I}} = \sigma_{A'\hat{X}_{\mathcal{I}}\mathcal{I}}$.

The second part of Alice takes A' as input and interacts with Bob in the rest of the protocol. To analyze the resulting joint output state $\tilde{\rho}_{A''CY^\ell}$, we can use the properties of weak string erasure, and let the second part of Alice interact with honest Bob starting from the state $\sigma_{A'\hat{X}^n\mathcal{I}}$. The protocol outputs a state $\tilde{\sigma}_{A''\hat{X}^nCY^\ell M}$, where M denotes all classical communication during the protocol. Note that the values Π, W_0^t, W_1^t, R_0 and R_1 can be computed from M. Let $S_i^\ell := \mathsf{Ext}(\Pi(\hat{\mathbf{Z}})_{\mathsf{Enc}(W_i^t)}, R_i)$ for $i \in \{0,1\}$, where for $(j,\alpha) \in [m] \times [\beta]$ we have $\hat{\mathbf{Z}}_{j,\alpha} := \hat{X}_{(j-1)\cdot\beta+\alpha}$. We obtain the state $\tilde{\sigma}_{A''S_0^\ell S_1^\ell CY^\ell}$ by taking the partial trace of $\tilde{\sigma}_{A''S_0^\ell S_1^\ell \hat{X}^n CY^\ell M}$. From the construction of this state and the fact that $\rho_{A'X_{\mathcal{I}}\mathcal{I}} = \sigma_{A'\hat{X}_{\mathcal{I}}\mathcal{I}}$ it follows directly that $\tilde{\rho}_{A''CY^\ell} = \tilde{\sigma}_{A''CY^\ell}$ and $\tilde{\sigma}_{A''S_0^\ell S_1^\ell CY^\ell} = \tilde{\sigma}_{A''S_0^\ell S_1^\ell CS_C^\ell}$. Hence

$$\tilde{\rho}_{A''CY^\ell} = \tilde{\sigma}_{A''CS_C^\ell} \ .$$

It remains to be shown that Alice does not learn anything about C, that is, $\tilde{\sigma}_{A''S_0^\ell S_1^\ell C} = \tilde{\sigma}_{A''S_0^\ell S_1^\ell} \otimes \tau_{\{0,1\}}$. From the properties of WSE it follows that $\sigma_{A'\hat{X}^n\mathcal{I}} = \sigma_{A'\hat{X}^n} \otimes \tau_{2^{[n]}}$. Since Bob randomly truncates/extends $\mathcal{I}$ such that $|\mathcal{I}| = n/4$, the resulting set $\mathcal{I}$ is also uniformly distributed over all subsets of size $n/4$ and independent of A'. Hence, conditioned on any fixed $W^t = w^t$, the permutation Π is uniform and independent of A'. It follows that the string W^t is also uniform and independent of A' and Π. From the properties of interactive hashing we are guaranteed that C is uniform and independent of Alice's view afterwards, and hence,

$$\tilde{\sigma}_{A''S_0^\ell S_1^\ell C} = \tilde{\sigma}_{A''S_0^\ell S_1^\ell} \otimes \tau_{\{0,1\}} \ .$$

$\square$

Second, we show that the protocol is secure against a cheating Bob. We again first give an intuitive argument. We have from weak string erasure that Bob gains only a limited amount of information about the string X^n. The properties of interactive hashing ensure that Bob has very little control over one of the subsets of blocks chosen by the interactive hashing. Therefore, by the results on min-entropy sampling, Bob has only limited information about the bits of X^n in these blocks. Privacy amplification can then be used to turn this into almost complete ingorance.

Lemma 5.4 (Security for Alice). *Protocol WSE-to-FROT satisfies security for Alice with an error of*

$$41 \cdot 2^{-\frac{\lambda^2}{512\omega^2\beta}n} + 2\varepsilon \ .$$

Proof. Let $\rho_{X^nB'}$ be the cq-state created by the execution of WSE. From the properties of WSE it follows that there exists a state $\sigma_{X^nB'}$ such that $\mathrm{H}_\infty(X^n|B')_\sigma \geq \lambda n$ and $\rho_{X^nB} \approx_\varepsilon \sigma_{X^nB'}$, which implies that

$$\mathrm{H}_\infty^\varepsilon(\mathbf{Z}|B')_\rho = \mathrm{H}_\infty^\varepsilon(X^n|B')_\rho \geq \lambda n \ .$$

Recall that our goal is to show that Bob has high min-entropy about the string X^n restricted to one of the subsets of blocks generated by the interactive hashing protocol. Our first step is to count the subsets of blocks which are bad for Alice in the sense that Bob has a lot of information about X^n in such blocks. We then show that the probability that both sets chosen via the interactive hashing primitive lie in the bad set of blocks is exponentially small in n.

First of all, note that the permutation Π is generated by Bob. In particular, if Bob is dishonest, Π may depend on his quantum information B'. This corresponds to the situation studied in Lemma 2.5. With Lemma 2.5, we therefore conclude that for the uniform[10] distribution over subsets $\mathcal{S} \subset [m]$ of size $m/4 = |\mathcal{S}|$

$$\Pr_{\mathcal{S}}\left[\mathrm{H}_\infty^{\varepsilon+4\delta}(\Pi(\mathbf{Z})_{\mathcal{S}}|\mathcal{S}\Pi B'') < \left(\frac{\omega-1}{\omega}\right)\frac{\lambda n}{4}\right] \leq \delta^2 \ , \tag{44}$$

---

[10]Note that, in the protocol, we do not actually sample from the uniform distribution over subsets; the bound (44) is merely used in a counting argument here to establish that the number of "bad" subsets is limited, cf. (45) below.

where $\delta = 2^{-m\lambda^2/(512\omega^2)}$ and B'' is Bob's part of the shared quantum state after he has sent Π to Alice. Let $\mathcal{B}ad$ be the set of all subsets of size $m/4$ that result in small min-entropy, i.e.,

$$\mathcal{B}ad := \left\{ \mathcal{S} \subseteq [m] \;\middle|\; |\mathcal{S}| = \frac{m}{4} \text{ and } \mathrm{H}_\infty^{\varepsilon+4\delta}(\Pi(\mathbf{Z})_\mathcal{S}|\mathcal{S}\Pi B'') < \left(\frac{\omega-1}{\omega}\right)\frac{\lambda n}{4} \right\} .$$

Since we have considered the uniform distribution over all subsets of size $m/4$, we conclude from (44) that

$$|\{ w^t \in \{0,1\}^t \mid \mathsf{Enc}(w^t) \in \mathcal{B}ad \}| \leq |\mathcal{B}ad| \leq \binom{m}{m/4}\delta^2 \leq 2 \cdot 2^t \delta^2. \tag{45}$$

In the first inequality, we have used the fact that Enc is injective, i.e., every element in the image has exactly one preimage. In the last inequality, we used the fact that $\binom{m}{m/4} \leq 2 \cdot 2^t$. By the third property of the interactive hashing, we conclude that

$$\Pr\left[\mathsf{Enc}(W_0^t) \in \mathcal{B}ad \text{ and } \mathsf{Enc}(W_1^t) \in \mathcal{B}ad \right] \leq 16 \frac{2 \cdot 2^t \delta^2}{2^t} \leq 32\delta^2 . \tag{46}$$

Let $\tilde\rho_{\mathbf{Z}W_0^t W_1^t \Pi B'''}$ be the shared quantum state after the interactive hashing, where B''' is Bob's part of that state. From (46) it follows that there exists a $C \in \{0,1\}$, or more precisely, there exists an ideal state $\tilde\sigma_{\mathbf{Z}W_0^t W_1^t \Pi B''' C}$ with $\tilde\rho_{\mathbf{Z}W_0^t W_1^t \Pi B'''} = \tilde\sigma_{\mathbf{Z}W_0^t W_1^t \Pi B'''}$, such that

$$\Pr_{\tilde\sigma}\left[\mathrm{H}_\infty^{\varepsilon+4\delta}(\Pi(\mathbf{Z})_{\mathsf{Enc}(W_{1-C}^t)}|W_0^t W_1^t \Pi B''')_{\tilde\sigma} \geq \left(\frac{\omega-1}{\omega}\right)\frac{\lambda n}{4} \right] \geq 1 - 32\delta^2 . \tag{47}$$

Note that Bob may use his quantum state during the interactive hashing, but he cannot increase the probability of (46) this way. Furthermore, any processing may only increase his uncertainty. Let $\mathcal{A}$ be the event that the inequality in the argument on the lhs. of (47) holds. Let

$$\tilde\sigma_{\mathbf{Z}W_0^t W_1^t \Pi B''' C R_0 R_1} := \tilde\sigma_{\mathbf{Z}W_0^t W_1^t \Pi B''' C} \otimes \tau_\mathcal{R} \otimes \tau_\mathcal{R}$$

and let S_0^ℓ and S_1^ℓ be calculated as stated in the protocol. Using the chain rule (see (16)) and the fact that (R_0, R_1) are independent, we get

$$\mathrm{H}_\infty^{\varepsilon+4\delta}(\Pi(\mathbf{Z})_{\mathsf{Enc}(W_{1-C}^t)}|S_C^\ell C R_0 R_1 W_0^t W_1^t \Pi B''', \mathcal{A})_{\tilde\sigma} \geq \left(\frac{\omega-1}{\omega}\right)\frac{\lambda n}{4} - \ell - 1 .$$

Using privacy amplification (Theorem 2.3), we then have conditioned on the event $\mathcal{A}$ that

$$\frac{1}{2}\|\tilde\sigma_{S_{1-C}, S_C C R_0 R_1 W_0^t W_1^t \Pi B'''} - \tau_{\{0,1\}^\ell} \otimes \tilde\sigma_{S_C C R_0 R_1 W_0^t W_1^t \Pi B'''}\|_1 \leq \delta + 2\varepsilon + 8\delta , \tag{48}$$

since

$$\left(\frac{\omega-1}{\omega}\right)\frac{n\lambda}{4} - 2\ell - 1 \geq 2\log 1/\delta = 2 \cdot \frac{\lambda^2 m}{512\omega^2} ,$$

which follows from

$$\ell \leq \left(\frac{\omega-1}{\omega}\right)\frac{\lambda n}{8} - \frac{\lambda^2 m}{512\omega^2} - \frac{1}{2} .$$

Let $B^* := (R_0 R_1 W_0^t W_1^t \Pi B''')$ be Bob's part in the output state. Since $\Pr[\mathcal{A}] \geq 1 - 32\delta^2$, we get

$$\tilde\sigma_{S_{1-C} S_C B^* C} \approx_{32\delta^2 + 9\delta + 2\varepsilon} \tau_{\{0,1\}^\ell} \otimes \tilde\sigma_{S_C B^* C}$$

and

$$\tilde\sigma_{S_0 S_1 B^*} = \tilde\rho_{S_0 S_1 B^*} .$$

Since $\delta^2 \leq \delta$, this implies the security condition for Alice, with a total error of at most $41\delta + 2\varepsilon$. $\qquad\square$

Finally, we show that the protocol is correct when Alice and Bob are both honest.

Lemma 5.5 (Correctness). *Protocol WSE-to-FROT satisfies correctness with an error of*

$$3 \cdot 2^{-\frac{1}{16}n} \leq 3 \cdot 2^{-\frac{\lambda^2}{512\omega^2\beta}n} \ .$$

Proof. Let $\xi := 2^{-n/16}$. We have to show that the state $\tilde{\rho}_{S_0^\ell S_1^\ell C Y^\ell}$ at the end of the protocol is 3ε-close to the given ideal state $\tilde{\sigma}_{S_0^\ell S_1^\ell C S_C^\ell}$. Using the Hoeffding bound [58], the probability that a random subset of $[n]$ has less than $n/4$ elements is at most $\exp(-n/8) \leq \xi$. Hence the probability that Bob has to pad s with 0s (which are likely to be incorrect) when both parties are honest is is at most ξ. Let $\mathcal{A}$ be the event that this does not happen. It remains to show that the state $\tilde{\rho}_{S_0^\ell S_1^\ell C Y^\ell | \mathcal{A}}$ is 2ξ-close to the given ideal state $\sigma_{S_0^\ell S_1^\ell C S_C^\ell}$. Note that the correctness condition of WSE ensures that the state created by WSE is equal to $\rho_{X^n \mathcal{I} X_\mathcal{I}} = \sigma_{X^n \mathcal{I} X_\mathcal{I}}$, where $\sigma_{X^n \mathcal{I}} = \tau_{\{0,1\}^n} \otimes \tau_{2^n}$. Since $\mathcal{I}_0$ and $\mathcal{I}_1$ are chosen independently of X^n, $X_{\mathcal{I}_0}$ and $X_{\mathcal{I}_1}$ are independent and have a min-entropy of $n/4$ each. Since $\ell \leq n/8 \leq n/4 - 2\log 1/\xi$, it follows from Theorem 2.3 that S_0^ℓ and S_1^ℓ are independent and each of them is ξ-close to uniform. Furthermore, by the same arguments as in Lemma 5.3 we have that C is uniform and independent of S_0^ℓ and S_1^ℓ. Hence,

$$\rho_{S_0^\ell S_1^\ell C | \mathcal{A}} \approx_{2\xi} \sigma_{S_0^\ell S_1^\ell C} \ .$$

Since the extra condition on the permutation Π implies that Bob can indeed calculate $\Pi(\mathbf{Z})_{\mathsf{Enc}(W)}$ from $X_\mathcal{I}$, we have that $Y^\ell = S_C^\ell$. Using $\Pr[\mathcal{A}] \geq 1 - \xi$, we get

$$\rho_{S_0^\ell S_1^\ell C Y^\ell} \approx_{3\xi} \sigma_{S_0^\ell S_1^\ell C S_C^\ell} \ .$$

Finally, $\lambda \leq 1$, $\beta > 1$ and $\omega \geq 2$ give us $1/16 > \lambda^2/(512\omega^2\beta)$ from which the claim follows. $\qquad\square$

6 Conclusions and open problems

We have shown that secure bit commitment and oblivious transfer can be obtained with unconditional security in the noisy-storage model. We have connected the security of our protocols to the information-carrying capacity of the noisy channel describing the malicious party's storage. We found a natural tradeoff between the (classical) capacity of the storage channel and the rates at which oblivious transfer and bit commitment can be performed: higher noise levels lead to stronger security.

While the connection between capacities of channels and security turns out to be directly applicable to a number of settings of practical interest, our work raises several immediate questions concerning the exact requirements for security in the noisy-storage model. Already now our work has sparked a number of new works. Our technique of relating security to a coding problem has been used to construct another, simpler, protocol for oblivious transfer [54], albeit at the expense of requiring significantly more noise in memory to achieve security. Other channels have been shown to satisfy the strong converse property, and hence lead to security in our model [24]. Alternate forms of weak string erasure using high dimensional states have been investigated using our techniques to show that in the limit of large n, security in bounded-storage model holds as long as a constant fraction of transmitted states is lost (i.e., $\nu < 1$) [40], and the security of an eavesdropper with a noisy memory device in QKD was investigated [6]. A practical implementation is in progress [20].

Extending security: Clearly, it is desirable to extend the security guarantee to a wider range of noisy channels. The limiting factor in obtaining security from a noisy storage described by $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$ was the fact that we require the sufficiency condition $C_\mathcal{N} \cdot \nu < 1/2$ to hold (see Corollary 1.2), where ν is the storage rate and $C_\mathcal{N}$ is the classical capacity of $\mathcal{N}$. The constant $1/2$ is a result of using BB84-states, and stems from a corresponding uncertainty relation using post-measurement information [41]. It is a natural question whether we can go beyond this bound using BB84-encodings.

For channels with small classical capacity, our work reduces security to proving a strong converse for coding. Of considerable practical interest are continuous-variable channels: our results are also applicable in this case, given a suitable bound on the information-carrying capacity.

A more challenging question is to extend security to entirely different classes of channels than considered here. Our results are currently restricted to channels without memory. Possibly the most important class of channels to which our results do not apply are those with high classical capacity. This includes for example the dephasing channel whose classical capacity is 1. Security tradeoffs for such a channel are known [28] for the case of individual storage attacks [62]. For the fully general case considered here, it is not a priori clear whether small classical capacity is a necessary condition for security: Our security proof overestimates the capabilities of the malicious party by expressing his power purely by his ability to preserve classical information. Completely different techniques may be required to address this question.

Another way to extend our security analysis is to combine our protocols with computationally secure protocols to achieve security if the adversary either has noisy quantum storage *or* is computationally bounded. This can be achieved by using *combiners* (see [26, 25, 46]). For oblivious transfer, the same can be achieved using the techniques of [8, 66, 12, 14], which only requires the use of a computationally secure bit commitment scheme.

Limits for security: We have found *sufficient* conditions for security in the noisy-storage model. For concrete channels, these conditions give regions in the plane parametrized by the storage rate and the noise level (cf. Figure 1) where security is achievable. Establishing outer bounds on the achievability region is an interesting open problem. Corresponding *necessary* conditions could become practically relevant as technology advances.

Note that when the adversarial player is restricted to individual storage attacks, the optimal attacks are known [55]. It is an open problem whether the fully general coherent attacks considered here actually reduce the achievability region. In contrast, both kinds of attacks are known to be equivalent in QKD [49].

Our work is merely a proof of principle. For practical realizations of our protocols, the following issues need to be addressed:

Efficiency: One can reduce the amount of classical computation and communication needed to execute our protocols by using techniques from derandomization. In particular, we could use the constant-round interactive hashing protocol and the efficient encoding of subsets from [19], randomness-efficient samplers (see e.g., [22]), and extractors (see e.g. [56, 35, 57]) instead of two-universal hash functions.

In practice, both the security parameter ε and the number ℓ of bits in the commitment or oblivious transfer are fixed constants. Savings in communication may then be obtained by using alternative uncertainty relations (i.e., generalizations of (18), which is tight [1] for $\varepsilon = 0$).

Composability: We have shown security of oblivious transfer and bit commitment with respect to security definitions that are motivated by composability considerations: This should ensure that the protocols remain secure even when executed many times e.g., sequentially. It is, however, an open problem to show formal composability in our model as has been done in the setting of bounded-storage [64, 21]. To this end, a nice composability framework for our setting needs to be established.

Robustness: We have considered an idealized setting where the operations of the honest parties are error-free. In particular, the communication channel connecting Alice and Bob was assumed to be noiseless. In real applications, both the BB84-state preparation by (honest) Alice, the communication, and the measurement of (honest) Bob will be affected by noise. To guarantee security even in such a setting, we can apply the error-correction techniques of [55]. However, it remains to determine the exact tradeoff between the amount of tolerable noise of the communication channel (parametrized e.g., by the bit error rate) and the amount of noise in the malicious player's storage device [13].

We conclude with a few speculative remarks on potential applications of our work. Note that, in contrast to key distribution, general two-party computation is also interesting at short (physical) distances. An example is the problem of secure identification [17], where Alice wants to identify herself to Bob (possibly an ATM machine) without ever giving her password away. Our approach could be extended to realize this primitive in a similar way as in [55]. It would be interesting to find a new and more efficient protocol based

directly on weak string erasure. The setting of secure identification is especially suitable for our model, since the short distance between Alice and Bob implies that their communication channel is essentially error-free. At such short range, we could also use visible light for which much better detectors exists than are presently used in quantum key distribution. Note that Alice only needs to carry a device capable of generating BB84-states and allowing her to enter her password on a keypad. This device does not need to store any information about Alice herself and hence each user could carry an identical device which is completely exchangeable among different (trusted) users at any time. In particular, this means means that Alice's password is not compromised even if the device is lost. Finally, note that Alice's technological requirements are minimal: She only needs a device capable of generating BB84-states. This could potentially be small enough to be carried on a key chain.

Acknowledgments

References

[1] M. Ballester, S. Wehner, and A. Winter. State discrimination with post-measurement information. *IEEE Transactions on Information Theory*, 54(9):4183–4198, 2008.

[2] D. Beaver. Precomputing oblivious transfer. In *Advances in Cryptology — EUROCRYPT '95*, volume 963 of *Lecture Notes in Computer Science*, pages 97–109. Springer-Verlag, 1995.

[3] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Proceedings of the 2nd TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406, 2005.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[5] C. H. Bennett, I. Devetak, A. Harrow, P. Show, and A. Winter. Quantum reverse shannon theorem. arXiv:0912.5537, 2009.

[6] A. Bocquet. In preparation. Workshop on Cryptography from Storage Imperfections, Recent work, Caltech, March 20–22, 2010.

[7] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, Nov 1995.

[8] C. H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology — CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer, 1992.

[9] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

[10] J. L. Carter and M. N. Wegman. Universal classes of hash functions (extended abstract). In *STOC '77: Proceedings of the ninth annual ACM symposium on theory of computing*, pages 106–112, New York, NY, USA, 1977. ACM.

[11] C. Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2455–2466, 1994.

[12] C. Crépeau, P. Dumais, D. Mayers, and L. Salvail. Computational collapse of quantum state with application to oblivious transfer. In *Theory of Cryptography Conference — TCC '04*, volume 2951 of *Lecture Notes in Computer Science*. Springer-Verlag, 2004.

[13] M. Curty, H. Lo, C. Schaffner, and S. Wehner. Implementing two-party protocols in the noisy-storage model. *Physical Review A*, 81:052336, 2010.

[14] I. Damgaard, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner. Improving the security of quantum protocols. In *Advances in Cryptology — CRYPTO '09*, Lecture Notes in Computer Science. Springer-Verlag, 2009.

[15] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 360–378. Springer-Verlag, 2007.

[16] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the Bounded-Quantum-Storage Model. In *Proceedings of 46th IEEE FOCS*, pages 449–458, 2005.

[17] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 342–359. Springer-Verlag, 2007.

[18] Y.Z. Ding. Oblivious transfer in the bounded storage model. In *Proceedings of CRYPTO' 01*, volume 2139 of *Lecture Notes in Computer Science*, pages 155–170, 2001.

[19] Y.Z. Ding, D. Harnik, A. Rosen and R. Shaltiel. Constant-Round Oblivious Transfer in the Bounded Storage Model. In *Proceedings of TCC '04*, volume 2951 of *Lecture Notes in Computer Science*, pages 446–472, 2004.

[20] C. Ervens. In preparation. Workshop on Cryptography from Storage Imperfections, Recent work, Caltech, March 20–22, 2010.

[21] S. Fehr and C. Schaffner. Composing quantum protocols in a classical environment. arXiv:0804.1059, 2008.

[22] O. Goldreich. A sample of samplers: A computational perspective on sampling. Technical report, ECCC TR–97–020, 1997. Available at http://www.eccc.uni-trier.de/eccc/.

[23] O. Goldreich and R. Vainish. How to solve any protocol problem - an efficiency improvement. In *Advances in Cryptology — CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 73–86. Springer, 1988.

[24] M. Hayashi. Personal communication with Andreas Winter. 2010.

[25] D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen. On robust combiners for oblivious transfer and other primitives. In *Advances in Cryptology — EUROCRYPT '05*, volume 3494 of *Lecture Notes in Computer Science*, pages 96–113, 2005.

[26] A. Herzberg. On tolerant cryptographic constructions. In *CT-RSA*, pages 172–190, 2005. full version on Cryptology ePrint Archive, eprint.iacr.org/2002/135.

[27] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the 21st ACM STOC*, pages 12–24, 1989.

[28] A. Kalev and S. Wehner. Personal communication. 2008.

[29] J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of 20th ACM STOC*, pages 20–31, 1988.

[30] C. King. Additivity for unital qubit channels. *Journal of Mathematical Physics*, 43:4641–4653, 2002.

[31] C. King. The capacity of the quantum depolarizing channel. *IEEE Transactions on Information Theory*, 49(1):221–229, 2003.

[32] R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. arXiv:0712.4291, 2007.

[33] R. König, R. Renner, A. Bariska, and U. Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98:140502, 2007.

[34] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. arXiv:0807.1338, 2008.

[35] R. König and B. Terhal. The bounded-storage model in the presence of a quantum adversary. *IEEE Transactions on Information Theory*, 54(2):749–762, 2008.

[36] R. König and S. Wehner. A strong converse for classical channel coding using entangled inputs. arXiv:0903.2838, 2009.

[37] H-K. Lo. Insecurity of quantum secure computations. *Physical Review A*, 56:1154, 1997.

[38] H-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410, 1997.

[39] H-K. Lo and H.F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. In *Proceedings of PhysComp96*, 1996. quant-ph/9605026.

[40] P. Mandayam and S. Wehner. In preparation. Workshop on Cryptography from Storage Imperfections, Recent work, Caltech, March 20–22, 2010.

[41] H. Maassen and J. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters*, 60(1103), 1988.

[42] U. Maurer. A provably-secure strongly-randomized cipher. In *Advances in Cryptology — EURO-CRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 361–373. Springer-Verlag, May 1990.

[43] U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.

[44] D. Mayers. The trouble with quantum bit commitment. quant-ph/9603015, 1996.

[45] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1997.

[46] R. Meier, B. Przydatek, and J. Wullschleger. Robuster combiners for oblivious transfer. In *Theory of Cryptography Conference — TCC '07*. Springer-Verlag, 2007.

[47] R. Ostrovsky, R. Venkatesan, and M. Yung. Fair games against an all-powerful adversary. In *AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 155–169, 1991.

[48] I. S. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[49] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 2005. quant-ph/0512258.

[50] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Proceedings of TCC 2005*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005.

[51] J. Sanchez-Ruiz. Optimal entropic uncertainty relation in two-dimensional hilbert space. *Physics Letters A*, 244:189–195, 1998.

[52] G. Savvides. *Interactive Hashing and reductions between Oblivious Transfer variants*. PhD thesis, McGill University, Montreal, 2007.

[53] C. Schaffner. *Cryptography in the Bounded-Quantum-Storage Model*. PhD thesis, University of Aarhus, 2007. http://arxiv.org/abs/0709.0289.

[54] C. Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. arXiv:1002.1495. Workshop on Cryptography from Storage Imperfections, Recent work, Caltech, March 20–22, 2010.

[55] C. Schaffner, B. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Information and Computation*, 9:0963–0996, 2009.

[56] R. Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

[57] A. Ta-Shma. Short seed extractors against quantum storage. 2008. quant-ph/0808.1994.

[58] W. Uhlmann. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, March 1963.

[59] S. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. In *Advances in Cryptology – CRYPTO '03*, Lecture Notes in Computer Science, pages 61–77. Springer, 2003.

[60] S. Wehner. *Cryptography in a Quantum World*. PhD thesis, University of Amsterdam, 2008. arXiv:0806.3483.

[61] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from noisy photonic storage. arxiv:0711.2895, 2007.

[62] S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

[63] S. Wehner and A. Winter. Higher entropic uncertainty relations for anti-commuting observables. *Journal of Mathematical Physics*, 49:062105, 2008.

[64] S. Wehner and J. Wullschleger. Composable security in the bounded-quantum-storage model. In *Proceedings of ICALP*, pages 604–615, 2008.

[65] S. Wiesner. Conjugate coding. *Sigact News*, 15(1), 1983.

[66] A. C.-C. Yao. Security of quantum protocols against coherent measurements. In *Proceedings of 20th ACM STOC*, pages 67–75, 1995.

A Proofs for min-entropy sampling

A.1 The parameters for sampling – proof of Lemma 2.4

For the proof of Lemma 2.4, we first recall the definition of a *sampler*:

Definition A.1. *An (m, ξ, γ)-averaging sampler is a probability distribution over subsets $\mathcal{S} \subset [m]$ with the property that for all $(\mu_1, \ldots, \mu_m) \in [0, 1]^m$ we have*

$$\Pr_{\mathcal{S}} \left[\frac{1}{|\mathcal{S}|} \sum_{i \in \mathcal{S}} \mu_i \leq \frac{1}{m} \sum_{i=1}^{m} \mu_i - \xi \right] \leq \gamma \ .$$

Choosing subsets of a fixed size at random is a prime example of a sampler; this is the sampler we will use. The parameters of this sampler are as follows

Lemma A.2. *Let $s < m$ and let $P_{\mathcal{S}}$ be the uniform distribution over subsets $\mathcal{S} \subset [m]$ of size $|\mathcal{S}| = s$. Then $P_{\mathcal{S}}$ is an $(m, \xi, 2^{-s\xi^2/2})$-sampler for every $s > 0$ and $\xi \in [0, 1]$.*

Proof. Fix $s > 0$ and $\xi \in [0, 1]$ In [32, Lemma 2.2], $P_{\mathcal{S}}$ was shown to be a $(m, \xi, e^{-s\xi^2/2})$-sampler. The claim then follows from the fact that $e^{-s\xi^2/2} \leq 2^{-s\xi^2/2}$. $\qquad\square$

Replacing $h_{\min}$ by H_∞, the following lemma follows directly from [32, Lemma 6.15 and Lemma 6.20]. The proof follows the same step as the proof of Theorem 6.18 in [32].

Lemma A.3. *Let $\rho_{Z^m Q}$ be a cq-state, where $Z^m = (Z_1, \ldots, Z_m)$ with $Z_i \in \{0,1\}^\beta$, and let $P_{\mathcal{S}}$ be an (m, ξ, γ)-averaging sampler supported on subsets $\mathcal{S}$ of size $s = |\mathcal{S}|$. Then*

$$\Pr \left[\frac{\mathrm{H}_\infty^{4\gamma^{1/4}}(Z_{\mathcal{S}}|\mathcal{S}Q)}{s\beta} \geq \frac{\mathrm{H}_\infty(Z^m|Q)}{m\beta} - c \right] \geq 1 - \sqrt{\gamma}$$

where

$$c = \frac{\log 1/\gamma}{2m\beta} + \xi + 2\kappa \log 1/\kappa$$

and $\kappa = \frac{m}{s\beta} \leq 0.15$.

We are now ready to give the

Proof of Lemma 2.4. Because of the definition of smooth min-entropy and the fact that partial traces do not increase distance, it suffices to establish the claim for $\varepsilon = 0$. By Lemma A.2 and Lemma A.3, we have

$$\Pr \left[\frac{\mathrm{H}_\infty^{4 \cdot 2^{-s\xi^2/8}}(Z_{\mathcal{S}}|\mathcal{S}Q)}{s\beta} \geq \frac{\mathrm{H}_\infty(Z^m|Q)}{m\beta} - c \right] \geq 1 - 2^{-s\xi^2/4} \qquad \text{where}$$
$$c = \frac{s\xi^2}{4m\beta} + \xi + 2\sqrt{\kappa} \tag{49}$$

if $\kappa = \frac{m}{s\beta} \leq 0.06$. Here we used the inequalities

$$\kappa \log 1/\kappa \leq \sqrt{\kappa} \qquad \text{for } \kappa \leq 0.06 \ ,$$
$$\beta \geq 1 \ , \qquad s \leq m \qquad \text{and} \qquad \xi \leq 1 \ .$$

Note that the condition $\kappa \leq 0.06$ is satisfied if $s \geq m/4$ and $\beta \geq 67$. Setting $\xi := \lambda/(4\omega)$ and using $s \geq m/4$ again, we get for $256\omega^2/\lambda^2 \leq \beta$ that

$$\begin{aligned}
c &\leq \frac{\lambda^2}{64\omega^2\beta} + \frac{\lambda}{4\omega} + 4\sqrt{\frac{1}{\beta}} \\
&\leq \frac{\lambda^4}{2^{14}\omega^4} + \frac{\lambda}{4\omega} + \frac{\lambda}{4\omega} \\
&\leq \frac{\lambda}{2\omega} + \frac{\lambda}{2\omega} = \frac{\lambda}{\omega}
\end{aligned}$$

In particular, this implies that

$$\frac{H_\infty(Z^m|Q)}{m\beta} - c \geq \lambda - c \geq \left(\frac{\omega-1}{\omega}\right)\lambda \,. \tag{50}$$

Combining (49), (50) with $s\xi^2 = s\lambda^2/(16\omega^2) \geq m\lambda^2/(64\omega^2)$ and $\delta = 2^{-m\lambda^2/(512\omega^2)}$ gives the claim. $\qquad\square$

A.2 Generalized min-entropy sampling – proof of Lemma 2.5

Proof. By definition of the smooth min-entropy, there exists a (possibly subnormalized) cq-state $\bar{\rho}_{\mathbf{Z}Q}$ with $\mathbf{Z} \in \mathbb{M}_{m\times\beta}(\{0,1\})$ such that

$$\frac{1}{2}\|\bar{\rho}_{\mathbf{Z}Q} - \rho_{\mathbf{Z}Q}\|_1 \leq \varepsilon$$

and

$$H_\infty(\mathbf{Z}|Q)_{\bar{\rho}} \geq \lambda \,. \tag{51}$$

By the monotonicity of the trace distance under CPTPMs, we therefore have

$$\frac{1}{2}\|\bar{\rho}_{\mathbf{Z}Q'\Pi} - \rho_{\mathbf{Z}Q'\Pi}\|_1 \leq \varepsilon \tag{52}$$

for the state $\bar{\rho}_{\mathbf{Z}Q'\Pi} := (\mathbb{I}_{\mathbf{Z}} \otimes \mathcal{E})(\bar{\rho}_{\mathbf{Z}Q})$, and by the fact that CPTPMs can only increase min-entropy (cf. (23)),

$$H_\infty(\mathbf{Z}|Q'\Pi)_{\bar{\rho}} \geq H_\infty(\mathbf{Z}|Q)_{\bar{\rho}} \,. \tag{53}$$

With (34) (applied to the conditional states $\bar{\rho}_{\mathbf{Z}Q'|\Pi=\pi}$), it is easy to see that

$$H_\infty(\Pi(\mathbf{Z})|Q'\Pi)_{\bar{\rho}} = H_\infty(\mathbf{Z}|Q'\Pi)_{\bar{\rho}} \,. \tag{54}$$

Combining (51), (53) and (54) gives

$$H_\infty(\Pi(\mathbf{Z})|Q'\Pi)_{\bar{\rho}} \geq \lambda \,.$$

Applying Lemma 2.4 to $\bar{\rho}_{\Pi(\mathbf{Z})Q'\Pi}$ (with $Q = Q'\Pi$, $\Pi(\mathbf{Z})$ instead of $\mathbf{Z}$ and $\varepsilon = 0$) therefore leads to

$$\Pr_{\mathcal{S}}\left[\frac{H_\infty^{4\delta}(\Pi(\mathbf{Z})_{\mathcal{S}}|Q'\Pi)_{\bar{\rho}}}{s\beta} \geq \left(\frac{\omega-1}{\omega}\right)\lambda\right] \geq 1 - \delta^2 \qquad \text{where } \delta = 2^{-m\lambda^2/(512\omega^2)} \,.$$

The claim follows from the monotonicity of the trace distance under CPTPMs and (52), since these imply

$$\frac{1}{2}\|\bar{\rho}_{\Pi(\mathbf{Z})_{\mathcal{S}}Q'\Pi} - \rho_{\Pi(\mathbf{Z})_{\mathcal{S}}Q'\Pi}\|_1 \leq \varepsilon$$

for every subset $\mathcal{S} \subset [m]$. $\qquad\square$